

IEC 62304 compliant Software Development for Medical devices using Container Hardening

Rajasegar Rajendhiran Shanthi
*Nova Leah, Dundalk, Co Louth,
& National College of Ireland
Dublin, Ireland*

Anita Finnegan
*Nova Leah,
Dundalk, Co Louth, Ireland*

Fergal McCaffery
*Nova Leah &
Regulatory Software Research Center,
(Lero)/Dundalk Institute of Technology,
Dundalk, Co Louth, Ireland*

Vikas Sahni
*School of Computing,
National College of Ireland,
Dublin, Ireland*



Background

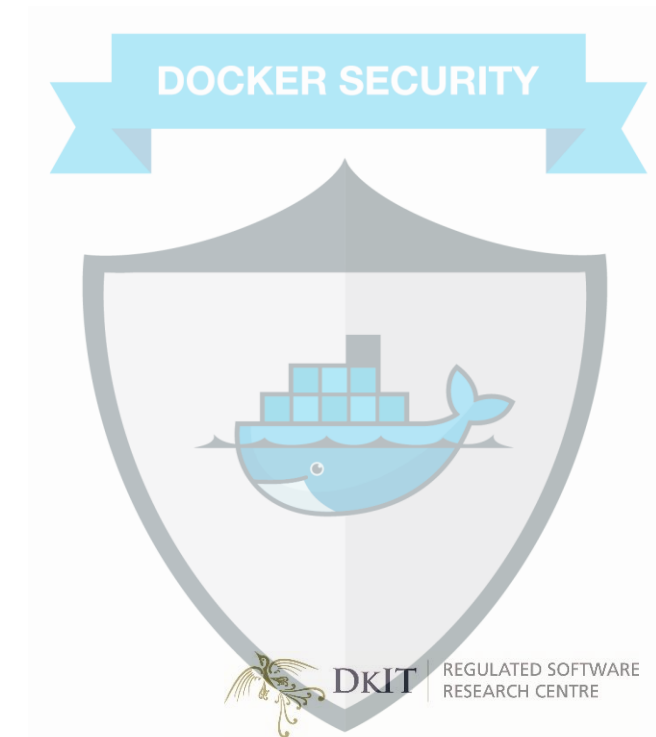
Security Assessment at Nova Leah Ltd.

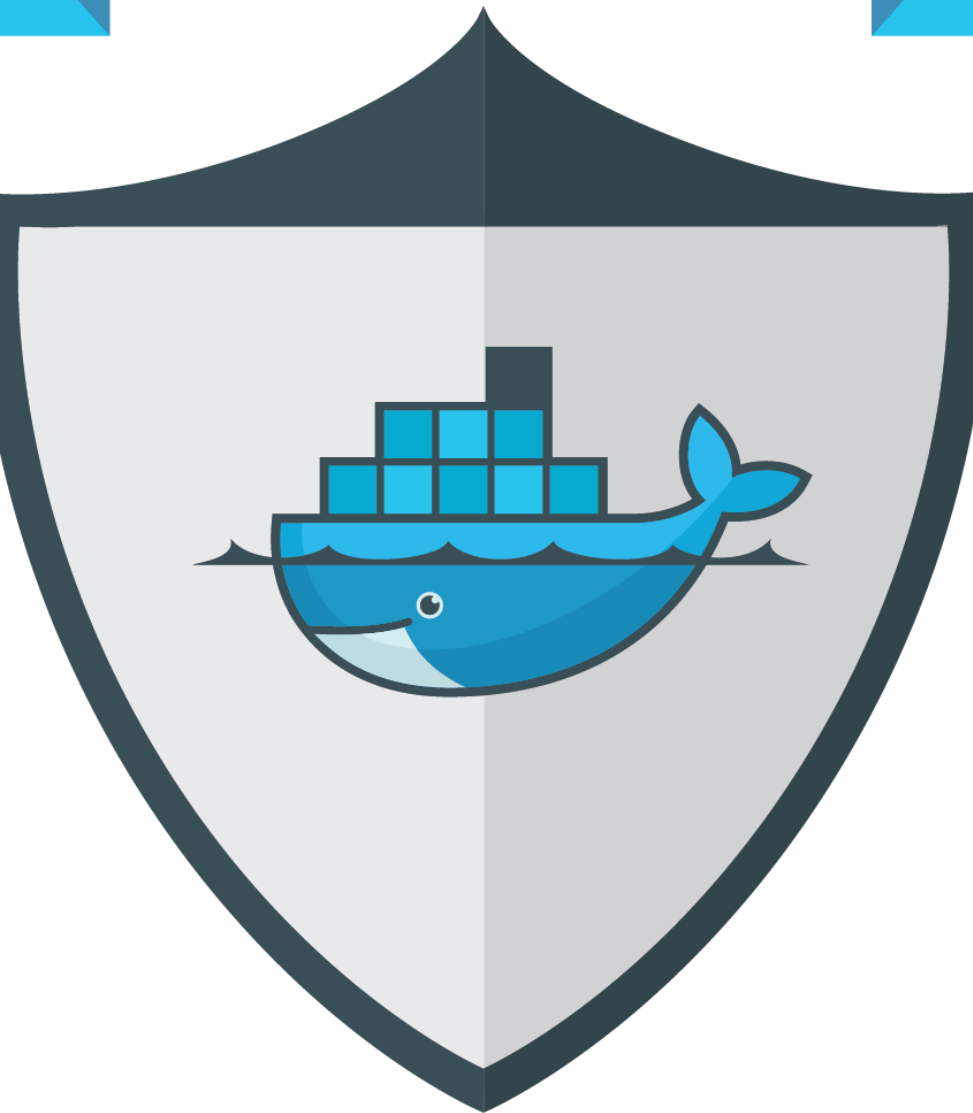
Internal Testing:

- Web Application Penetration Testing

Research Area:

- Docker Container security





Problem Identified

- Container Security: Hardening Containers
- Research Question: How can container-based applications used in medical device software development be hardened.

Literature Review

Focus of the literature review was on articles:

- Docker Container Vulnerabilities and Attacks
- Container Security
- Medical Device Software Lifecycle Regulation and Containerization

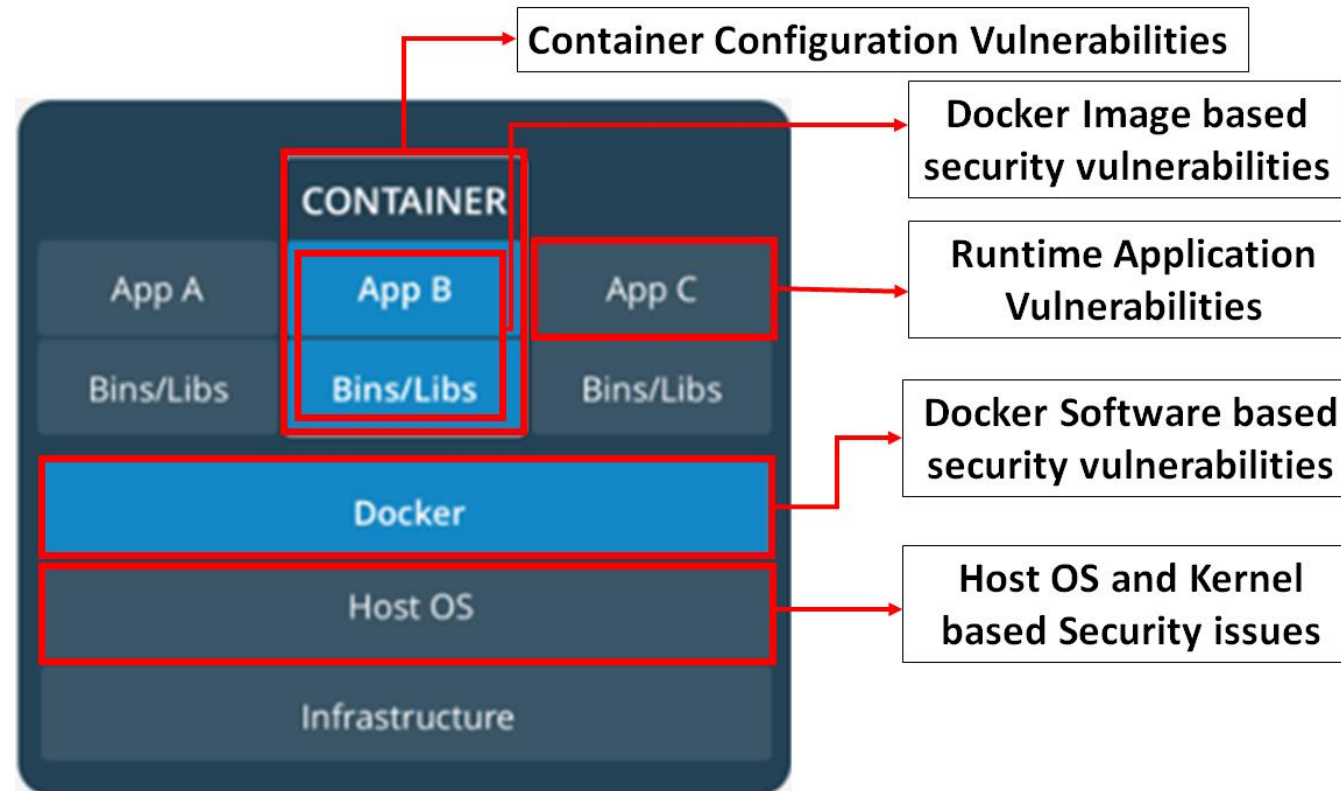
Literature Review:

Significant Paper :

Container-Based Clinical Solutions for Portable and Reproducible Image Analysis: Journal of Digital Imaging (2018)

- Research paper published by (Matelsky, J., Kiar, G., Johnson, E., Rivera, C., Toma, M., & Gray-Roncal, W. 2018) Containers and their use in the medical imaging industries as the complexity and computational requirements for the analysis are increasing.
- Use case: Integrating Docker as a containerization platform into a Clinical workflow.
- This article did not discuss security and regulatory compliance in Container based clinical solutions which is the key area for this research work.

Container Security Vulnerabilities and Threats

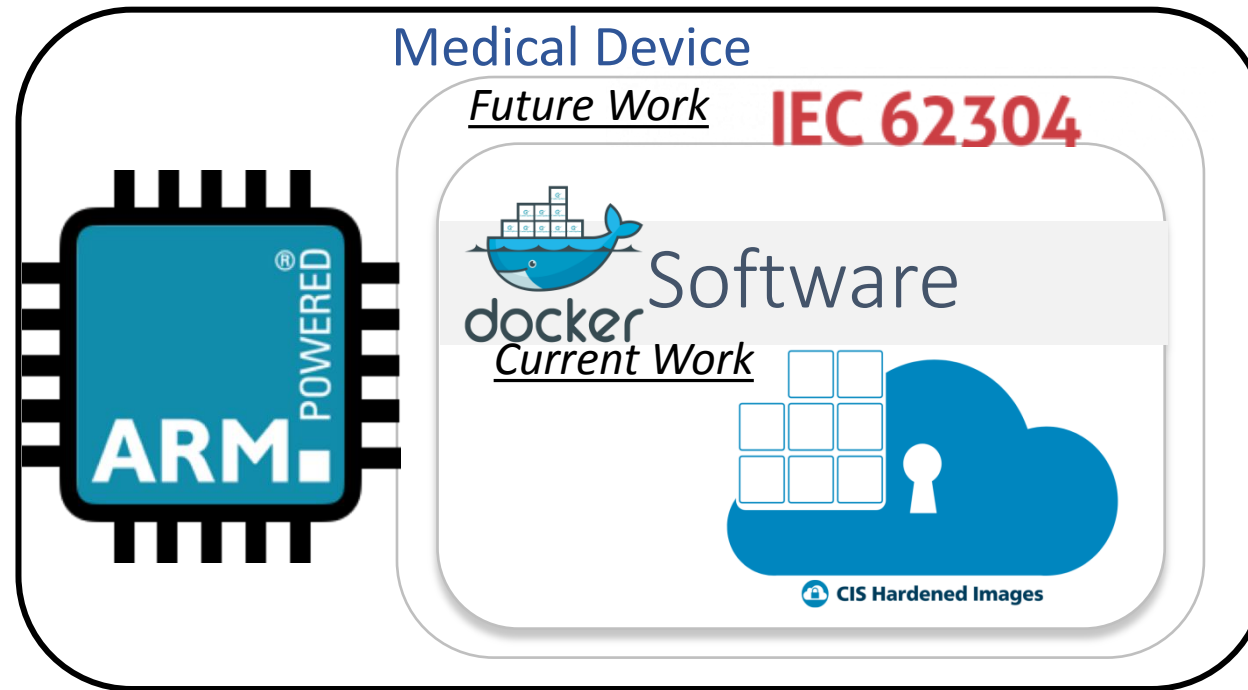


Action Research Methodology: Container Security

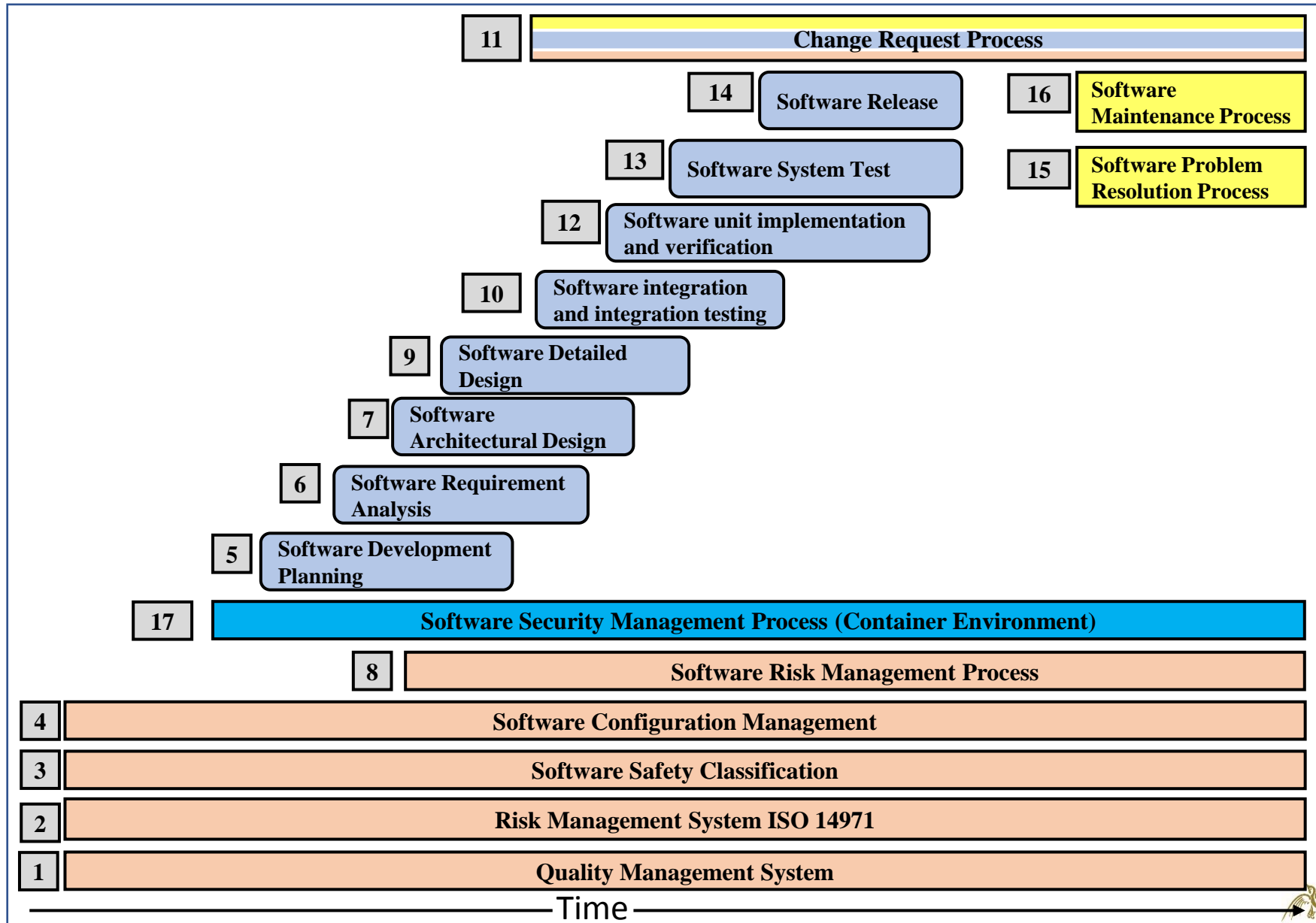


1. Container Security
2. Hardening Containers
3. Scanned results
4. Manual analysis using Standard benchmarks.
5. Provide the 1st iteration of solution to developers.
6. Feedback from development team for performing 2nd iteration.

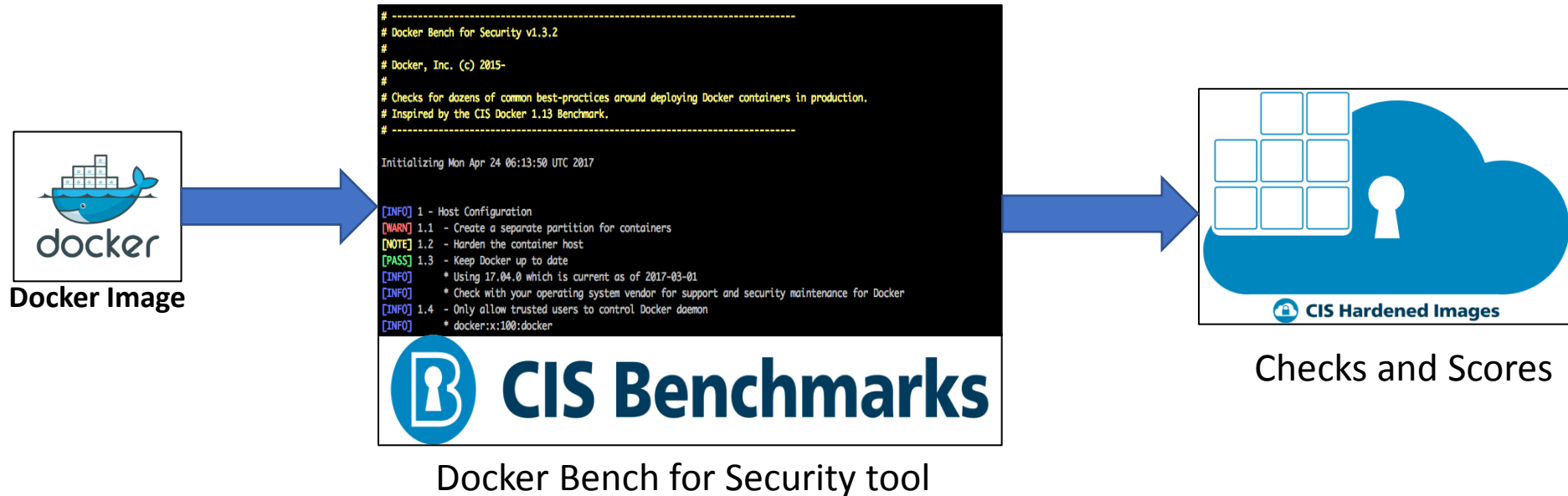
Implementation Container Hardening Flow



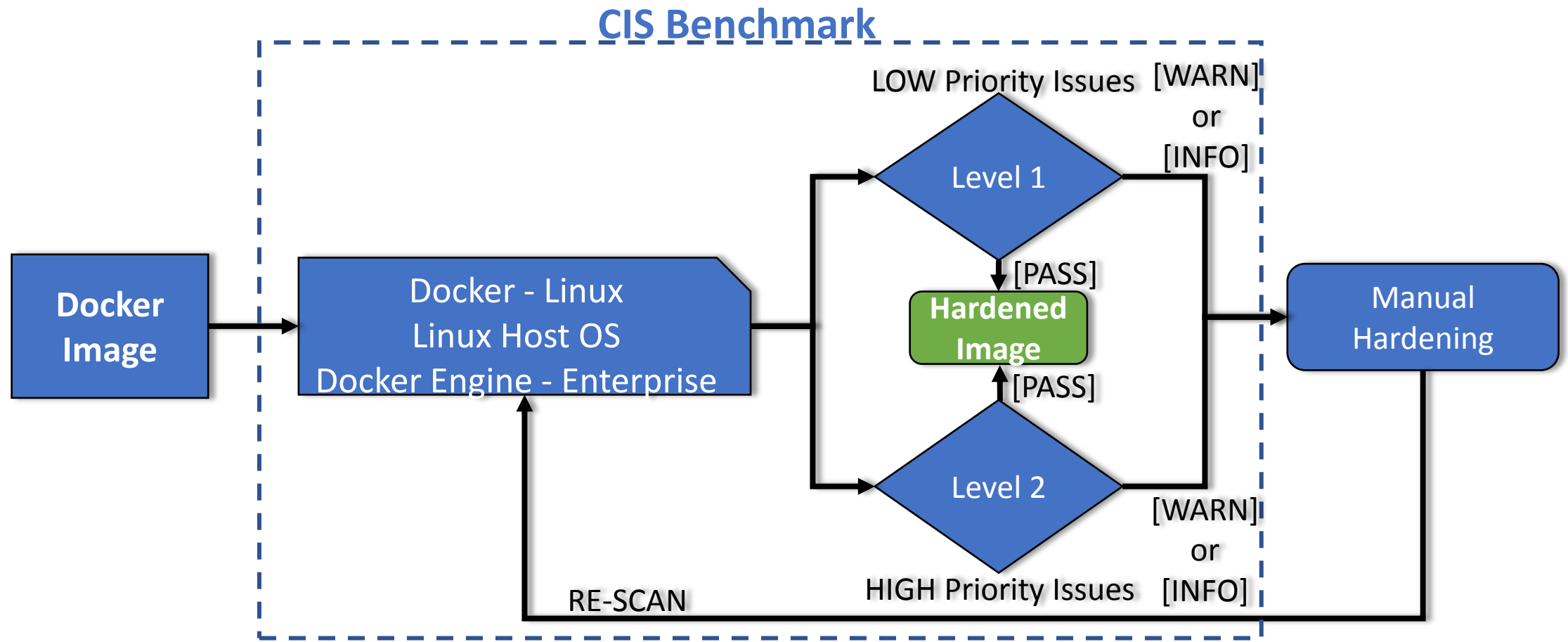
Updated Roadmap for IEC 62304:




CIS Benchmark Docker bench for security tool



CIS Benchmark: Docker bench for security tool



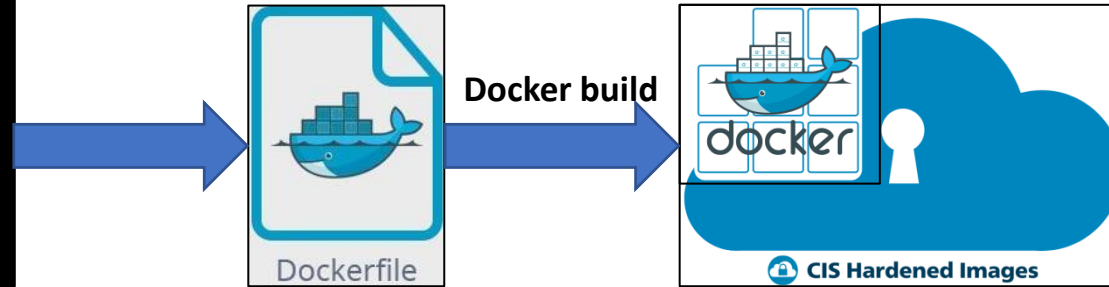
Implementing Container Hardening Flow



CIS Benchmarks

```
#-----  
# Docker Bench for Security v1.3.2  
#  
# Docker, Inc. (c) 2015-  
#  
# Checks for dozens of common best-practices around deploying Docker containers in production.  
# Inspired by the CIS Docker 1.13 Benchmark.  
#-----  
  
Initializing Mon Apr 24 06:13:50 UTC 2017  
  
[INFO] 1 - Host Configuration  
[WARN] 1.1 - Create a separate partition for containers  
[NOTE] 1.2 - Harden the container host  
[PASS] 1.3 - Keep Docker up to date  
[INFO] * Using 17.04.0 which is current as of 2017-03-01  
[INFO] * Check with your operating system vendor for support and security maintenance for Docker  
[INFO] 1.4 - Only allow trusted users to control Docker daemon  
[INFO] * docker:x:100:docker
```

CIS Docker Benchmark guidelines



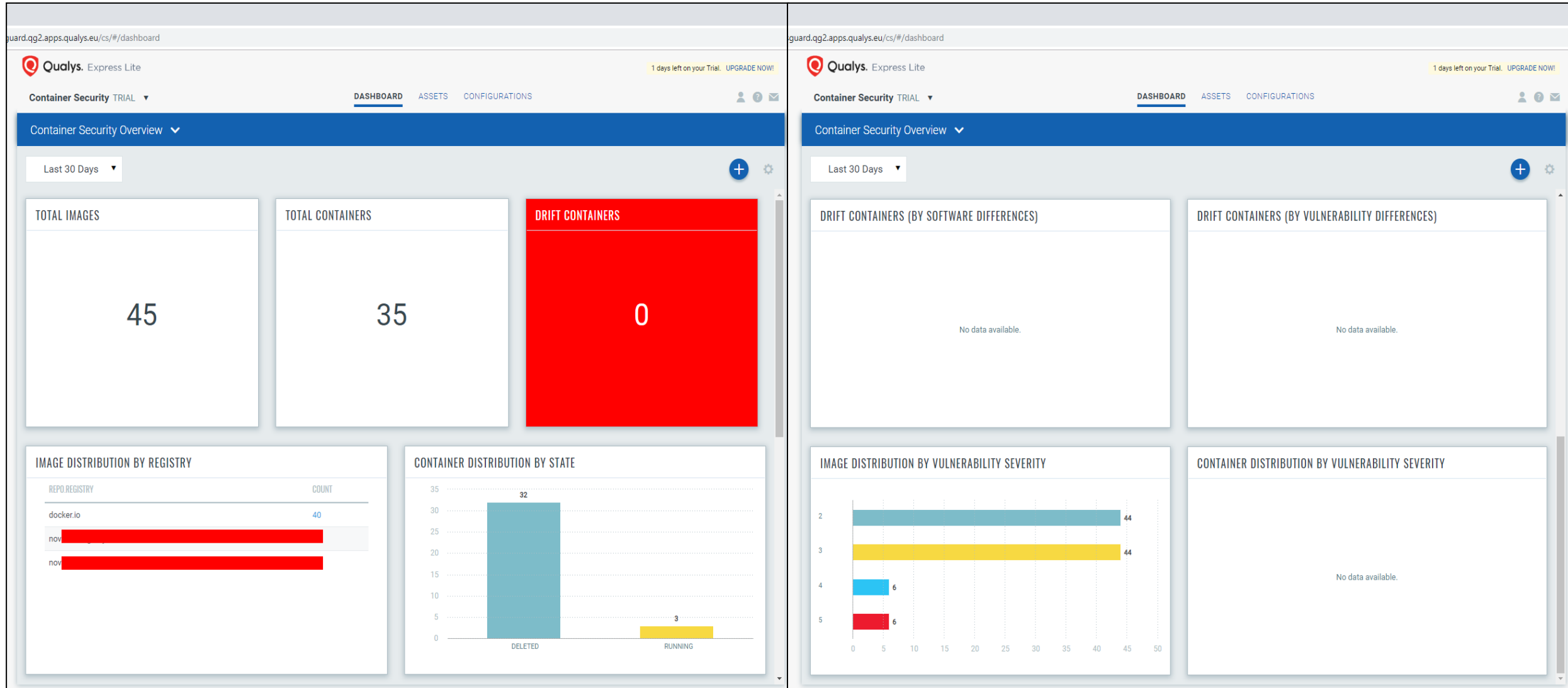
Dockerfile with
Hardening
parameters

Hardened
Docker Image

Hardening Actions Performed

Sl. No.	Hardening Actions Performed
1	<ul style="list-style-type: none">➤ Update NGINX system and base system➤ Add custom user profile and setup home directory.➤ Add-in post installation file for providing permissions➤ Make sure system dirs are owned by root and not writable by anybody else.➤ Disable password login for everybody.
2	<ul style="list-style-type: none">➤ Removed apk configs. by commented out as it is needed for apk to install other stuff, temp shadow, passwd, group and selective admin commands.➤ Removed world-writable permissions except for /tmp/, unnecessary accounts, excluding current app user and root, interactive login shell for everybody.
3	<ul style="list-style-type: none">➤ Removed the following functions and packages: suid & sgid files, dangerous commands, init scripts since we do not use, kernel tunables, root home dir, fstab, any symlinks that we broke during previous steps.

Container Scan using Qualys Container Scanner



Docker Auditing and Hardening Demo tool



Docker Auditing and Hardening Tool V1.1

- Go to the tool directory “ICT Solution docker_tool_tv4_FINAL CODE”/
Run this command “./mscript_v2.sh”.

```
-----  
NOVA LEAH Ltd.
```

```
DOCKER Auditing and Hardening tool V1.1  
-----
```

1. Show the currently running Docker Images and other checks
2. Show all available Docker Images
3. Checks for old docker image versions and removes
4. Build New Docker Image
5. CIS Benchmark security test Score
6. ADD MORE Functionalities HERE

1. Show the current running Docker Images & Checks

```
NOVA LEAH Ltd.
DOCKER Auditing and Hardening tool V1.1
-----
1. Show the currently running Docker Images and other checks
2. Show all available Docker Images
3. Checks for old docker image versions and removes
4. Build New Docker Image
5. CIS Benchmark security test Score
6. ADD MORE Functionalities HERE
1

<-----2.9 Ensure the default cgroup usage has been confirmed /2.10/2.11----->
Audited:
root      1029      1    0 Aug16 ?      00:04:09 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
root      1818     1816    0 18:45 pts/0    00:00:00 grep dockerd

<-----2.12 Ensure centralized and remote logging is configured----->
json-file
root      1029      1    0 Aug16 ?      00:04:09 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
root      1833     1816    0 18:46 pts/0    00:00:00 grep dockerd

<-----2.15 Ensure that a daemon-wide custom seccomp profile is applied if appropriate----->
[name=apparmor name=seccomp,profile=default]

<-----4.5 Ensure Content trust for Docker is Enabled----->
The value should be 1

<-----4.11 Ensure only verified packages are are installed----->
REPOSITORY          TAG          IMAGE ID          CREATED          SIZE
<none>              <none>       58365ec9b516     4 days ago      8.86MB
raj                 tg           dd8f08b8837b     4 days ago      6.75MB

test1_image         tag          c7b3ee836225     6 days ago      7.04MB
quay.io/coreos/clair-git  latest      ee65e681b999     2 weeks ago     55.7MB
alpine              3.10.0       4d90542f0623     2 months ago    5.58MB

tomcat              8-jre8       3639174793ba     3 months ago    463MB
mariadb             10.2         453efb22c1c9     3 months ago    346MB
quay.io/coreos/clair  latest      79f851f41934     5 months ago    355MB
alpine              3.2          98f5f2d17bd1     6 months ago    5.27MB
docker/docker-bench-security  latest      0037349aef7e     7 months ago    51.6MB

Testing this script
CONTAINER ID      IMAGE          COMMAND          CREATED          STATUS          PORTS          NAMES
```

1. Figure 1

1. Show the current running Docker Images & Checks

Testing this script

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
REPOSITORY	TAG	IMAGE ID	CREATED	SIZE		
<none>	<none>	58365ec9b516	4 days ago	8.86MB		
raj	tq	dd8f08b8837b	4 days ago	6.75MB		
test1_image	tag	c7b3ee836225	6 days ago	7.04MB		
quay.io/coreos/clair-git	latest	ee65e681b999	2 weeks ago	55.7MB		
alpine	3.10.0	4d90542f0623	2 months ago	5.58MB		
tomcat	8-jre8	3639174793ba	3 months ago	463MB		
mariadb	10.2	453efb22c1c9	3 months ago	346MB		
quay.io/coreos/clair	latest	79f851f41934	5 months ago	355MB		
alpine	3.2	98f5f2d17bd1	6 months ago	5.27MB		
docker/docker-bench-security	latest	0037349aef7e	7 months ago	51.6MB		

1. Figure 2

```
docker: 'containers' is not a docker command.
See 'docker --help'

<-----5.2 Ensure that, if applicable, SELinux security options are set (Scored)----->
2afae34aadee5eb8ff20fe5eef430765398998468837978a7c3f4ba4bdala610: SecurityOpt=[label=disable]
fdf222fea0082fa900e25ae331745fb0cd118f556bb960dd8dd1632b53d3acc5: SecurityOpt=[label=disable]
60886f497bfee4708e1797d7dbbcea69815f88f7d33f7ac06b43982fa9e55e2a: SecurityOpt=<no value>
502d8bb1115278900b81d09f0900adbc93d4f0cca485e823056a2e73d033be52: SecurityOpt=<no value>
0d93fbaa84b9a33edc38138f385bc0df8ac60b32183f8a35ef45850d880582b2: SecurityOpt=<no value>
c3c7735dd97aa1e6e774f4e280d110204089ae4ae65aa64cdfdfdd4ee6183788: SecurityOpt=<no value>
14f77910d885bec6610bf0f1a2cbf5017d1dcd9955d6b695d46f75728fd73f69: SecurityOpt=<no value>
558bbe4e8bb3a6a0cc6fd806a90513e4433fa28bbac529f65ff1b0ba6c5a84c1: SecurityOpt=<no value>
3930d0049cbf81980b32471c3e5a104337a03ff248c7eea827bf09afaad85f1e: SecurityOpt=<no value>

<-----5.6 Ensure sshd is not run within containers----->
60886f497bfe
502d8bb11152
0d93fbaa84b9

<-----5.7 Ensure privileged ports are not mapped within containers (Scored)----->
60886f497bfee4708e1797d7dbbcea69815f88f7d33f7ac06b43982fa9e55e2a: Ports=map[80/tcp:[map[HostIp:0.0.0.0 HostPort:80]]]
502d8bb1115278900b81d09f0900adbc93d4f0cca485e823056a2e73d033be52: Ports=map[3306/tcp:<nil>]
0d93fbaa84b9a33edc38138f385bc0df8ac60b32183f8a35ef45850d880582b2: Ports=map[8080/tcp:<nil>]

THANKS FOR USING DOCKER Auditing and Hardening tool V1.1
```

2. Show all available Docker Images

```
-----
THANKS FOR USING DOCKER Auditing and Hardening tool V1.1
-----
root@ [REDACTED] docker_tool_tv4# ./mscript_v2.sh
-----
NOVA LEAH Ltd.
DOCKER Auditing and Hardening tool V1.1
-----
1. Show the currently running Docker Images and other checks
2. Show all available Docker Images
3. Checks for old docker image versions and removes
4. Build New Docker Image
5. CIS Benchmark security test Score
6. ADD MORE Functionalities HERE
2
REPOSITORY                                TAG                                IMAGE ID                            CREATED                            SIZE
<none>                                    <none>                            4c15c820314e                       4 days ago                        8.86MB
<none>                                    <none>                            58365ec9b516                       4 days ago                        8.86MB
<none>                                    <none>                            9347d6ce8c7e                       4 days ago                        8.86MB
<none>                                    <none>                            af4c470eb5f5                       4 days ago                        8.86MB
<none>                                    <none>                            baa46af3d39a                       4 days ago                        8.86MB
<none>                                    <none>                            11650e1c4583                       4 days ago                        8.86MB
<none>                                    <none>                            a133d52cb0ae                       4 days ago                        8.86MB
<none>                                    <none>                            c86f735ca97f                       4 days ago                        8.86MB
<none>                                    <none>                            7a687a9e1ab7                       4 days ago                        8.86MB
<none>                                    <none>                            0d83b3680720                       4 days ago                        8.86MB
<none>                                    <none>                            2f15577078d7                       4 days ago                        8.86MB
<none>                                    <none>                            e62b16c2ea47                       4 days ago                        8.86MB
<none>                                    <none>                            42e1c98097d1                       4 days ago                        8.86MB
<none>                                    <none>                            7b2893692f55                       4 days ago                        8.86MB
<none>                                    <none>                            8c1088f20d62                       4 days ago                        8.86MB
<none>                                    <none>                            d6d50b724898                       4 days ago                        8.86MB
<none>                                    <none>                            a9de2b912b0e                       4 days ago                        8.86MB
<none>                                    <none>                            2a095a1beb88                       4 days ago                        8.86MB
<none>                                    <none>                            44ad7295c571                       4 days ago                        8.86MB
<none>                                    <none>                            f5a170bd7590                       4 days ago                        6.75MB
<none>                                    <none>                            e96b90ada9f2                       4 days ago                        5.27MB
<none>                                    <none>                            f707e8f1ead7                       4 days ago                        5.27MB
<none>                                    <none>                            c73afc290dde                       4 days ago                        5.27MB
<none>                                    <none>                            84dd6957d0c3                       4 days ago                        5.27MB
raj                                       tg                                dd8f08b8837b                       4 days ago                        6.75MB
<none>                                    <none>                            4c660c2c36de                       4 days ago                        6.75MB
<none>                                    <none>                            15ff5f1360a6                       4 days ago                        6.75MB
<none>                                    <none>                            a2683fcca5d5                       4 days ago                        6.75MB
<none>                                    <none>                            71521d5465a3                       4 days ago                        5.27MB
-----
test1_image                             tag                                c7b3ee836225                       6 days ago                        7.04MB
<none>                                    <none>                            974799872c08                       6 days ago                        7.04MB
```

2. Figure 1

2. Show all available Docker Images

2. Figure 2

```
<none>                <none>                7a687a9e1ab7          4 days ago          8.86MB
<none>                <none>                0d83b3680720          4 days ago          8.86MB
<none>                <none>                2f15577078d7          4 days ago          8.86MB
<none>                <none>                e62b16c2ea47          4 days ago          8.86MB
<none>                <none>                42e1c98097d1          4 days ago          8.86MB
<none>                <none>                7b2893692f55          4 days ago          8.86MB
<none>                <none>                8c1088f20d62          4 days ago          8.86MB
<none>                <none>                d6d50b724898          4 days ago          8.86MB
<none>                <none>                a9de2b912b0e          4 days ago          8.86MB
<none>                <none>                2a095a1beb88          4 days ago          8.86MB
<none>                <none>                44ad7295c571          4 days ago          8.86MB
<none>                <none>                f5a170bd7590          4 days ago          6.75MB
<none>                <none>                e96b90ada9f2          4 days ago          5.27MB
<none>                <none>                f707e8f1ead7          4 days ago          5.27MB
<none>                <none>                c73afc290dde          4 days ago          5.27MB
<none>                <none>                84dd6957d0c3          4 days ago          5.27MB
raj                  tg                  dd8f08b8837b          4 days ago          6.75MB
<none>                <none>                4c660c2c36de          4 days ago          6.75MB
<none>                <none>                15ff5f1360a6          4 days ago          6.75MB
<none>                <none>                a2683fcca5d5          4 days ago          6.75MB
<none>                <none>                71521d5465a3          4 days ago          5.27MB
-----
test1_image          tag                  c7b3ee836225          6 days ago          7.04MB
<none>                <none>                974799872c08          6 days ago          7.04MB
<none>                <none>                1f5dfac8fbf3          6 days ago          7.04MB
<none>                <none>                68a57bc29e25          6 days ago          7.04MB
<none>                <none>                58de9e4afefe          6 days ago          7.04MB
<none>                <none>                4e80ca99815e          6 days ago          7.04MB
<none>                <none>                27154a408250          6 days ago          7.04MB
<none>                <none>                b1a036d097e3          6 days ago          7.04MB
<none>                <none>                a34e94779fcb          6 days ago          7.04MB
<none>                <none>                699dab34ef45          6 days ago          7.04MB
<none>                <none>                2efbc396e4f0          6 days ago          7.04MB
<none>                <none>                086800eb996e          6 days ago          5.58MB
quay.io/coreos/clair-git latest              ee65e681b999          2 weeks ago         55.7MB
alpine               3.10.0              4d90542f0623          2 months ago        5.58MB
-----
tomcat                8-jre8              3639174793ba          3 months ago         463MB
mariadb               10.2                453efb22c1c9          3 months ago         346MB
quay.io/coreos/clair  latest              79f851f41934          5 months ago         355MB
alpine                3.2                 98f5f2d17bd1          6 months ago         5.27MB
docker/docker-bench-security latest              0037349aef7e          7 months ago         51.6MB
-----
THANKS FOR USING DOCKER Auditing and Hardening tool V1.1
-----
```

3. Show all available Docker Images

3. Figure 1

```
-----
NOVA LEAH Ltd.
DOCKER Auditing and Hardening tool V1.1
-----

1. Show the currently running Docker Images and other checks
2. Show all available Docker Images
3. Checks for old docker image versions and removes
4. Build New Docker Image
5. CIS Benchmark security test Score
6. ADD MORE Functionalities HERE
3
This Tool will check for the Old versions of Docker Images & Delete it

Docker is out of date! To update: yum -y install docker-engine

All containers are stopped.
2afae34aadee
fdf222fea008
60886f497bfe
502d8bb11152
0d93fbbaa84b9
c3c7735dd97a
14f77910d885
558bbe4e8bb3
3930d0049cbf

Deleting old containers ..

Deleting untagged containers ..
Deleted: sha256:58365ec9b5164aa8ccd320c873162851d1046bead363d0fda3dfc0f2c6b42650
Deleted: sha256:4c15c820314ebe3487bc1d75acb8f2bae4f27e97133e244582b3a27de3669981
Deleted: sha256:9347d6ce8c7e0969ed38c26da5dfe840f3a2b2d4d4c034114963a36df073f676
Deleted: sha256:15de2609288b1fd02b6366ebf3da0319ba8602122d1cdaef2463c2fd943edb79
Deleted: sha256:af4c470eb5f58dceb51d9f6c5409ee090bc9b3247093431021d1c64a2085f59e
Deleted: sha256:41e112d76eebe281de832b39d40fb8dd242c6e78619c26db80a54d1cd16687fa
Deleted: sha256:b4a46af3d39abd81a43dbe5c0bc95b73878ffec171ec4bf7c80eadf97505c96e
Deleted: sha256:5bbdba657579c19d2fc6a80da53ba517b33e86223cdea7c6fcac09f4e73cde9f
Deleted: sha256:11650e1c4583854936b9bce931d2470ed0b6adad6ef48d015b70fbf65e2ec0e0
Deleted: sha256:ba1452cfd8c3bd237dfeec99bfbdbf89341be44f01dc697ba8e654f914d93ba5d
Deleted: sha256:a133d52cb0aeeb4a0a6a6d00ca37d316d21ca77ae82c264a8d0803a5f0130cb4
Deleted: sha256:01aa9954331101663922a1cb1b95b6d5d70488398a381640710530cd2dd74a42
Deleted: sha256:c86f735ca97f6158c9eb1662569b5bc60a2983f2e99c5df259032372eec54136
Deleted: sha256:d8012ab075a65c2d7ed1dd813b54c6968639fc7f681e1881222ac71922f88734
Deleted: sha256:7a687a9e1ab7257ff28329c3d0d51cb64f05dc75a949587baccfc6570abfbd5
Deleted: sha256:803d245fd3f398661a6e7aef23b9dcf2a1105671735aa1010ce28a695310dc6f
Deleted: sha256:0d83b3680720cfc4d1b5c4e6354e8ba650de6354f69932354c891881d80b8782
Deleted: sha256:9d5d53968220e4c4c39aaa63db7e7252efb5e59c86e27b15110f19d49d753a5c
Deleted: sha256:2f15577078d74dab4baf4130df1a5dc5f715dfb1f5617df66134dbdb8cf6b64a
```


3. Show all available Docker Images

3. Figure 2

```
Deleted: sha256:01aa9954331101663922a1cb1b95b6d5d70488398a381640710530cd2dd74a42
Deleted: sha256:c86f735ca97f6158c9eb1662569b5bc60a2983f2e99c5df259032372eec54136
Deleted: sha256:d8012ab075a65c2d7ed1dd813b54c6968639fc7f681e1881222ac71922f88734
Deleted: sha256:7a687a9e1ab7257ff28329c3d0d51cb64f05dc75a949587baccfc6570abfbdb5
Deleted: sha256:803d245fd3f398661a6e7aef23b9dcf2a1105671735aa1010ce28a695310dc6f
Deleted: sha256:0d83b3680720cfc4dlb5c4e6354e8ba650de6354f69932354c891881d80b8782
Deleted: sha256:9d5d53968220e4c4c39aaa63db7e7252efb5e59c86e27b15110f19d49d753a5c
Deleted: sha256:2f15577078d74dab4baf4130df1a5dc5f715dfb1f5617df66134dbdb8cf6b64a
Deleted: sha256:0bdae91df31ac181d3eab8299ce33f29ab73851be6ed2b8d36966f8faef626e8
Deleted: sha256:e62b16c2ea47b0f784f83a3d4f9843b081d1b44b1a9167e73f114043b4710045
Deleted: sha256:42e1c98097d1c8a0e0eeffb0538144c3b5364be36c44599f3da47cc17b167b237
Deleted: sha256:c962740fc62bf9e8933b1393db8d5803fcc570d7350bef70d558acbed78f340a
Deleted: sha256:7b2893692f554c0ee266377a075b2b75bdb3d130f68e2b4c8787c898c04a500a
Deleted: sha256:a1713ee922725821fc07c2a37378e7940ce64355798a165bd02bb45a3d69a377
Deleted: sha256:8c1088f20d629fd4fcc99aca2ca18e03458618b6a31e8957829671399ae5aff3
Deleted: sha256:eb68e967feb7f87fc7922d7905cbddac689689de80cb8cec0a7150a24d6ada3bd
Deleted: sha256:d6d50b7248980c69be12fbc543c8a5996accdd63650ec5110223f2671cd59ef5
Deleted: sha256:2b2fc0483c763b2da82c5c32fd84cb0645bbad50c05cb7493b075e93cce163fb
Deleted: sha256:a9de2b912b0ed7b044fe8ea6ce8cddd9b4479fca752783c587b183234f2b2557
Deleted: sha256:2392b690f61cc4c5b5dfb62a7494dfd85c582d9ecc82f5032fd8dclbf86fbf52
Deleted: sha256:2a095a1beb8835d11aa0c7343fc28d19b2be681f41a9077fe258459a7780c3f3
Deleted: sha256:3ca1c27576ad53f7a67165e5bd199be1944a1641c6e4aecf72466dce679e6789
Deleted: sha256:44ad7295c571e28342c5a724736d3989b4d6ef1cdc156a237d626cdc6244e00d
Deleted: sha256:2279be09a572b5d01437bf2b872e53f1821cb8c02a5281e371c942c4c009ca2f
Deleted: sha256:f5a170bd7590daf7f8b3ee339f91d3c05888de33247a70104c87342ba35f6e47
Deleted: sha256:70ef345374fe3252a660f079773bcacc908e24c5ba0a9eee566e43e8347ead0f
Deleted: sha256:e96b90ada9f2e69a34e9a6d1a01452e085a9813753715b56c96b91c13cdb2684
Deleted: sha256:f707e8f1ead7151c84f9eff50e7dc12a7779f702b9ea93e30d776c432629a8fc
Deleted: sha256:84dd6957d0c365b799e6a137e4e92a2a5426a71bd196235188551a44e6d90d94
Deleted: sha256:c73afc290dde6a89ecb322313b91b4f5af88efdb94b215fe5ce77812f55f921c

Adding audit rules...

Enabling client-side signature integrity..

Starting Registry Daemon as v2.

Changing permissions for Docker service..
chmod: cannot access '/usr/lib/systemd/system/docker.service': No such file or directory

Security options and CPU & RAM restrictions are activated..
Container initializing..
docker: invalid reference format.
See 'docker run --help'.

-----
THANKS FOR USING DOCKER Auditing and Hardening tool V1.1
-----
```

4. Build New Docker Image

4. Figure 1

```
NOVA LEAH Ltd.
DOCKER Auditing and Hardening tool V1.1
-----
1. Show the currently running Docker Images and other checks
2. Show all available Docker Images
3. Checks for old docker image versions and removes
4. Build New Docker Image
5. CIS Benchmark security test Score
6. ADD MORE Functionalities HERE
4
<-----Select the below Image build Options----->
1. Build Docker Image with Alpin and Ngnix
2. Build Hardening Docker Image with Alpin and Ngnix
3. ADD MORE Image build Functionalities HERE
1
Type Docker name: [image]: raj
Type Docker Tag: [tag]: tag1
Sending build context to Docker daemon  4.096kB
Step 1/6 : FROM alpine:3.10.0
--> 98f5f2d17bd1
Step 2/6 : MAINTAINER Raja <@gmail.com>
--> Using cache
--> 71521d5465a3
Step 3/6 : RUN apk add --update nginx && rm -rf /var/cache/apk/*
--> Using cache
--> a2683fcca5d5
Step 4/6 : COPY nginx.conf /etc/nginx/nginx.conf
--> Using cache
--> 15ff5f1360a6
Step 5/6 : COPY index.html /usr/share/nginx/html/index.html
--> Using cache
--> 4c660c2c36de
Step 6/6 : CMD ["nginx", "-g", "daemon off;"]
--> Using cache
--> dd8f08b8837b
Successfully built dd8f08b8837b
Successfully tagged raj:tag1
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
raj	tag1	dd8f08b8837b	4 days ago	6.75MB
raj	tg	dd8f08b8837b	4 days ago	6.75MB
<none>	<none>	15ff5f1360a6	4 days ago	6.75MB
<none>	<none>	4c660c2c36de	4 days ago	6.75MB
<none>	<none>	a2683fcca5d5	4 days ago	6.75MB
<none>	<none>	71521d5465a3	4 days ago	5.27MB
test1_image	tag	c7b3ee836225	6 days ago	7.04MB
<none>	<none>	1f5dfac8fbf3	6 days ago	7.04MB
<none>	<none>	974799872c08	6 days ago	7.04MB

4. Build New Docker Image

4. Figure 2

```
Step 3/6 : RUN apk add --update nginx && rm -rf /var/cache/apk/*
----> Using cache
----> a2683fcca5d5
Step 4/6 : COPY nginx.conf /etc/nginx/nginx.conf
----> Using cache
----> 15ff5f1360a6
Step 5/6 : COPY index.html /usr/share/nginx/html/index.html
----> Using cache
----> 4c660c2c36de
Step 6/6 : CMD ["nginx", "-g", "daemon off;"]
----> Using cache
----> dd8f08b8837b
```

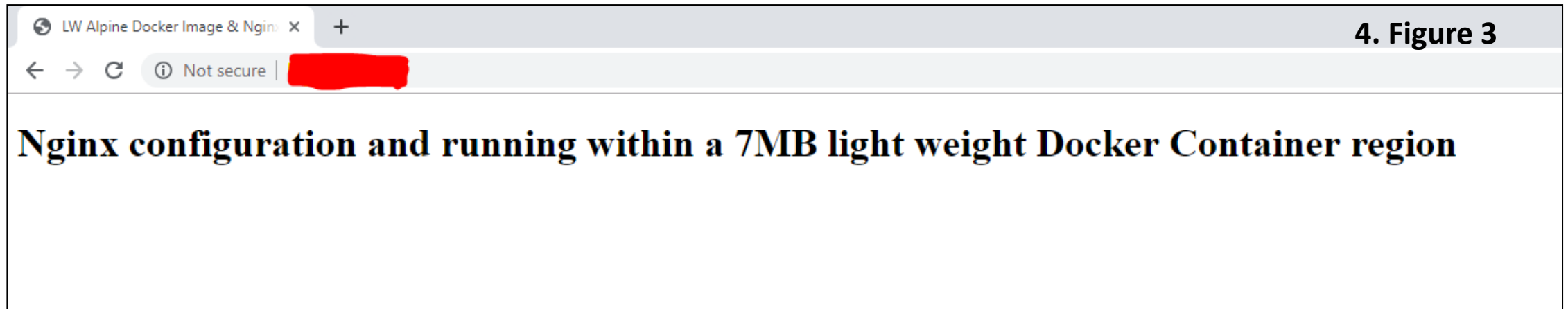
Successfully built dd8f08b8837b

Successfully tagged raj:tag1

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
raj	tag1	dd8f08b8837b	4 days ago	6.75MB
raj	tg	dd8f08b8837b	4 days ago	6.75MB
<none>	<none>	15ff5f1360a6	4 days ago	6.75MB
<none>	<none>	4c660c2c36de	4 days ago	6.75MB
<none>	<none>	a2683fcca5d5	4 days ago	6.75MB
<none>	<none>	71521d5465a3	4 days ago	5.27MB
test1_image	tag	c7b3ee836225	6 days ago	7.04MB
<none>	<none>	1f5dfac8fbf3	6 days ago	7.04MB
<none>	<none>	974799872c08	6 days ago	7.04MB
<none>	<none>	68a57bc29e25	6 days ago	7.04MB
<none>	<none>	58de9e4afefe	6 days ago	7.04MB
<none>	<none>	4e80ca99815e	6 days ago	7.04MB
<none>	<none>	27154a408250	6 days ago	7.04MB
<none>	<none>	b1a036d097e3	6 days ago	7.04MB
<none>	<none>	a34e94779fcb	6 days ago	7.04MB
<none>	<none>	699dab34ef45	6 days ago	7.04MB
<none>	<none>	2efbc396e4f0	6 days ago	7.04MB
<none>	<none>	086800eb996e	6 days ago	5.58MB
quay.io/coreos/clair-git	latest	ee65e681b999	2 weeks ago	55.7MB
alpine	3.10.0	4d90542f0623	2 months ago	5.58MB
tomcat	8-jre8	3639174793ba	3 months ago	463MB
mariadb	10.2	453efb22c1c9	3 months ago	346MB
quay.io/coreos/clair	latest	79f851f41934	5 months ago	355MB
alpine	3.2	98f5f2d17bd1	6 months ago	5.27MB
docker/docker-bench-security	latest	0037349aef7e	7 months ago	51.6MB

4. Build New Docker Image: Server started

- The command used to run the Nginx server is:
`$ docker run -p 80:8080 <Image_Name:tag>`



5. Docker bench for security

5. Figure 1

```
NOVA LEAH Ltd.
DOCKER Auditing and Hardening tool V1.1
-----
1. Show the currently running Docker Images and other checks
2. Show all available Docker Images
3. Checks for old docker image versions and removes
4. Build New Docker Image
5. CIS Benchmark security test Score
6. ADD MORE Functionalities HERE
5
sudo: unable to resolve host selenium
# -----
# 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 Mon Aug 26 18:53:19 IST 2019

[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 18.09.6, 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:999
[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
[INFO] 1.9 - Ensure auditing is configured for Docker files and directories - docker.socket
[INFO] * File not found
[WARN] 1.10 - Ensure auditing is configured for Docker files and directories - /etc/default/docker
[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
```

5. Docker bench for security

5. Figure 2

```
[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
[PASS] 2.17 - Ensure experimental features are avoided in production
[WARN] 2.18 - Ensure containers are restricted from acquiring new privileges

[INFO] 3 - Docker daemon configuration files
[INFO] 3.1 - Ensure that docker.service file ownership is set to root:root
[INFO] * File not found
[INFO] 3.2 - Ensure that docker.service file permissions are set to 644 or more restrictive
[INFO] * File not found
[INFO] 3.3 - Ensure that docker.socket file ownership is set to root:root
[INFO] * File not found
[INFO] 3.4 - Ensure that docker.socket file permissions are set to 644 or more restrictive
[INFO] * File not found
[PASS] 3.5 - Ensure that /etc/docker directory ownership is set to root:root
[PASS] 3.6 - Ensure that /etc/docker directory permissions are set to 755 or more restrictive
[INFO] 3.7 - Ensure that registry certificate file ownership is set to root:root
[INFO] * Directory not found
[INFO] 3.8 - Ensure that registry certificate file permissions are set to 444 or more restrictive
[INFO] * Directory not found
[INFO] 3.9 - Ensure that TLS CA certificate file ownership is set to root:root
[INFO] * No TLS CA certificate found
[INFO] 3.10 - Ensure that TLS CA certificate file permissions are set to 444 or more restrictive
[INFO] * No TLS CA certificate found
[INFO] 3.11 - Ensure that Docker server certificate file ownership is set to root:root
[INFO] * No TLS Server certificate found
[INFO] 3.12 - Ensure that Docker server certificate file permissions are set to 444 or more restrictive
[INFO] * No TLS Server certificate found
[INFO] 3.13 - Ensure that Docker server certificate key file ownership is set to root:root
[INFO] * No TLS Key found
```

5. Docker bench for security

5. Figure 3

```
[INFO] 3.14 - Ensure that Docker server certificate key file permissions are set to 400
[INFO] * No TLS Key found
[PASS] 3.15 - Ensure that Docker socket file ownership is set to root:docker
[PASS] 3.16 - Ensure that Docker socket file permissions are set to 660 or more restrictive
[INFO] 3.17 - Ensure that daemon.json file ownership is set to root:root
[INFO] * File not found
[INFO] 3.18 - Ensure that daemon.json file permissions are set to 644 or more restrictive
[INFO] * File not found
[PASS] 3.19 - Ensure that /etc/default/docker file ownership is set to root:root
[PASS] 3.20 - Ensure that /etc/default/docker file permissions are set to 644 or more restrictive

[INFO] 4 - Container Images and Build File
[INFO] 4.1 - Ensure a user for the container has been created
[INFO] * No containers running
[NOTE] 4.2 - Ensure that containers use trusted base images
[NOTE] 4.3 - Ensure unnecessary packages are not installed in the container
[NOTE] 4.4 - Ensure images are scanned and rebuilt to include security patches
[WARN] 4.5 - Ensure Content trust for Docker is Enabled
[WARN] 4.6 - Ensure HEALTHCHECK instructions have been added to the container image
[WARN] * No Healthcheck found: [raj:tag1 raj:tg]
[WARN] * No Healthcheck found: [raj:tag1 raj:tg]
[WARN] * No Healthcheck found: [novaleahtestregistry.azurecr.io/se_web:develop]
[WARN] * No Healthcheck found: [test1_image:tag]
[WARN] * No Healthcheck found: [quay.io/coreos/clair-git:latest]
[WARN] * No Healthcheck found: [alpine:3.10.0]
[WARN] * No Healthcheck found: [novaleahregistry.azurecr.io/se_web:1.19.8.azure]
[WARN] * No Healthcheck found: [tomcat:8-jre8]
[WARN] * No Healthcheck found: [mariadb:10.2]
[WARN] * No Healthcheck found: [quay.io/coreos/clair-git:latest]
[WARN] * No Healthcheck found: [alpine:3.2]
[WARN] * No Healthcheck found: [novaleahse/pdf_converter:latest novaleahregistry.azurecr.io/pdf_converter:v1]
[WARN] * No Healthcheck found: [novaleahse/pdf_converter:latest novaleahregistry.azurecr.io/pdf_converter:v1]
[INFO] 4.7 - Ensure update instructions are present in Dockerfile
[INFO] * Update instruction found: [raj:tag1 raj:tg]
[INFO] * Update instruction found: [raj:tag1 raj:tg]
[INFO] * Update instruction found: [novaleahtestregistry.azurecr.io/se_web:develop]
[INFO] * Update instruction found: [novaleahse/pdf_converter:latest novaleahregistry.azurecr.io/pdf_converter:v1]
[INFO] * Update instruction found: [tomcat:8-jre8]
[INFO] * Update instruction found: [mariadb:10.2]
[INFO] * Update instruction found: [novaleahse/pdf_converter:latest novaleahregistry.azurecr.io/pdf_converter:v1]
[INFO] * Update instruction found: [novaleahse/pdf_converter:latest novaleahregistry.azurecr.io/pdf_converter:v1]
[NOTE] 4.8 - Ensure setuid and setgid permissions are used in Dockerfile
[INFO] 4.9 - Ensure COPY is used instead of ADD in Dockerfile
[INFO] * ADD in image history: [raj:tag1 raj:tg]
[INFO] * ADD in image history: [raj:tag1 raj:tg]
[INFO] * ADD in image history: [novaleahtestregistry.azurecr.io/se_web:develop]
[INFO] * ADD in image history: [test1_image:tag]
```

5. Docker bench: Server stopped Checks and Score

5. Figure 4

```
[INFO] 4.9 - Ensure COPY is used instead of ADD in Dockerfile
[INFO] * ADD in image history: [raj:tag1 raj:tg]
[INFO] * ADD in image history: [raj:tag1 raj:tg]
[INFO] * ADD in image history: [novaleantestregistry.azurecr.io/se_web:develop]
[INFO] * ADD in image history: [test1 image:tag]
[INFO] * ADD in image history: [quay.io/coreos/clair-git:latest]
[INFO] * ADD in image history: [alpine:3.10.0]
[INFO] * ADD in image history: [novaleahregistry.azurecr.io/se_web:1.19.8.azure]
[INFO] * ADD in image history: [tomcat:8-jre8]
[INFO] * ADD in image history: [mariadb:10.2]
[INFO] * ADD in image history: [quay.io/coreos/clair:latest]
[INFO] * ADD in image history: [alpine:3.21]
[INFO] * ADD in image history: [docker/centos:7]
[INFO] * ADD in image history: [novaleanse/pdf_converter:latest novaleanregistry.azurecr.io/pdf_converter:v1]
[INFO] * ADD in image history: [novaleahse/pdf_converter:latest novaleahregistry.azurecr.io/pdf_converter:v1]
[NOTE] 4.10 - Ensure secrets are not stored in Dockerfiles
[NOTE] 4.11 - Ensure verified packages are only Installed

[INFO] 5 - Container Runtime
[INFO] * No containers running, skipping Section 5

[INFO] 6 - Docker Security Operations
[INFO] 6.1 - Avoid image sprawl
[INFO] * There are currently: 12 images
[INFO] 6.2 - Avoid container sprawl
[INFO] * There are currently a total of 10 containers, with 1 of them currently running

[INFO] 7 - Docker Swarm Configuration
[PASS] 7.1 - Ensure swarm mode is not Enabled, if not needed
[PASS] 7.2 - Ensure the minimum number of manager nodes have been created in a swarm (Swarm mode not enabled)
[PASS] 7.3 - Ensure swarm services are binded to a specific host interface (Swarm mode not enabled)
[PASS] 7.4 - Ensure data exchanged between containers are encrypted on different nodes on the overlay network
[PASS] 7.5 - Ensure Docker's secret management commands are used for managing secrets in a Swarm cluster (Swarm mode not enabled)
[PASS] 7.6 - Ensure swarm manager is run in auto-lock mode (Swarm mode not enabled)
[PASS] 7.7 - Ensure swarm manager auto-lock key is rotated periodically (Swarm mode not enabled)
[PASS] 7.8 - Ensure node certificates are rotated as appropriate (Swarm mode not enabled)
[PASS] 7.9 - Ensure CA certificates are rotated as appropriate (Swarm mode not enabled)
[PASS] 7.10 - Ensure management plane traffic has been separated from data plane traffic (Swarm mode not enabled)

[INFO] Checks: 74
[INFO] Score: 10
-----
THANKS FOR USING DOCKER Auditing and Hardening tool V1.1
-----
```

5. Docker bench: Server started Checks and Score

5. Figure 5

```
[PASS] 5.30 - Ensure the host's user namespaces is not shared
[PASS] 5.31 - Ensure the Docker socket is not mounted inside any containers

[INFO] 6 - Docker Security Operations
[INFO] 6.1 - Avoid image sprawl
[INFO]      * There are currently: 12 images
[INFO] 6.2 - Avoid container sprawl
[INFO]      * There are currently a total of 11 containers, with 4 of them currently running

[INFO] 7 - Docker Swarm Configuration
[PASS] 7.1 - Ensure swarm mode is not Enabled, if not needed
[PASS] 7.2 - Ensure the minimum number of manager nodes have been created in a swarm (Swarm mode not enabled)
[PASS] 7.3 - Ensure swarm services are bound to a specific host interface (Swarm mode not enabled)
[PASS] 7.4 - Ensure data exchanged between containers are encrypted on different nodes on the overlay network
[PASS] 7.5 - Ensure Docker's secret management commands are used for managing secrets in a Swarm cluster (Swarm mode not enabled)
[PASS] 7.6 - Ensure swarm manager is run in auto-lock mode (Swarm mode not enabled)
[PASS] 7.7 - Ensure swarm manager auto-lock key is rotated periodically (Swarm mode not enabled)
[PASS] 7.8 - Ensure node certificates are rotated as appropriate (Swarm mode not enabled)
[PASS] 7.9 - Ensure CA certificates are rotated as appropriate (Swarm mode not enabled)
[PASS] 7.10 - Ensure management plane traffic has been separated from data plane traffic (Swarm mode not enabled)

[INFO] Checks: 105
[INFO] Score: 13

-----
THANKS FOR USING DOCKER Auditing and Hardening tool V1.1
-----
```


CIS Docker Benchmark Scoring System

Checks are assessed based on success and failure compliances with the following scoring statuses:

- “Scored” recommendations.
- “Not Scored” recommendations.

Scored	Not Scored
89	27
Success Compliance – Impacts Benchmark Score	Success Compliance – Does not Impact Benchmark Score
Failure Compliance – Impacts Benchmark Score	Failure Compliance – Does not Impact Benchmark Score

6. Options to Add more functions to the tool

```
NOVA LEAH Ltd.
```

6. Figure 1

```
DOCKER Auditing and Hardening tool V1.1
```

- ```

1. Show the currently running Docker Images and other checks
2. Show all available Docker Images
3. Checks for old docker image versions and removes
4. Build New Docker Image
5. CIS Benchmark security test Score
6. ADD MORE Functionalities HERE
```

```
4
```

```
<-----Select the below Image build Options-----
```

- ```
1. Build Docker Image with Alpin and Ngnix  
2. Build Hardening Docker Image with Alpin and Ngnix  
3. ADD MORE Image build Functionalities HERE
```

```
3
```

```
ADD New Docker Image build Functionalities
```

```
-----  
THANKS FOR USING DOCKER Auditing and Hardening tool V1.1  
-----
```


Conclusion and Future Works

Current Work:

- Proving Container security to organization's Development region
- Container Security through hardening technique using In-House tool

Future Work:

- Implementing IEC 62304 (MEDICAL DEVICE SOFTWARE - SOFTWARE LIFE CYCLE PROCESSES)
- Implement Regulatory compliance within Docker Images
- Adaptable in other industries software development process (i.e Automobile)





This paper is supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 732242 (DEIS project).