# docker 취약점 진단 프로젝트





E-01 정보시스템 취약점 진단

표재경 (팀장) 김서연 김효민 전동현 황유림

### 목 차

1 도커 소개

2 악성 Docker 이미지 배포 및 Docker 취약성 사례 3 Docker 진단 항목 수립

> 4 진단 환경 소개

> > 5 수동 진단

6 자동 스크립트 진단

Docker 취약점 상세 보고서

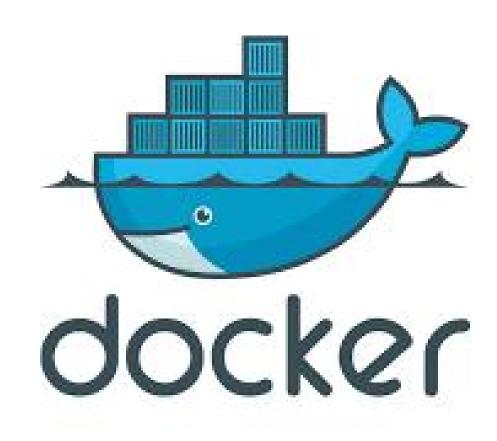
8 기대<u>효</u>과

9 인사이트



# 1. Docker 소개

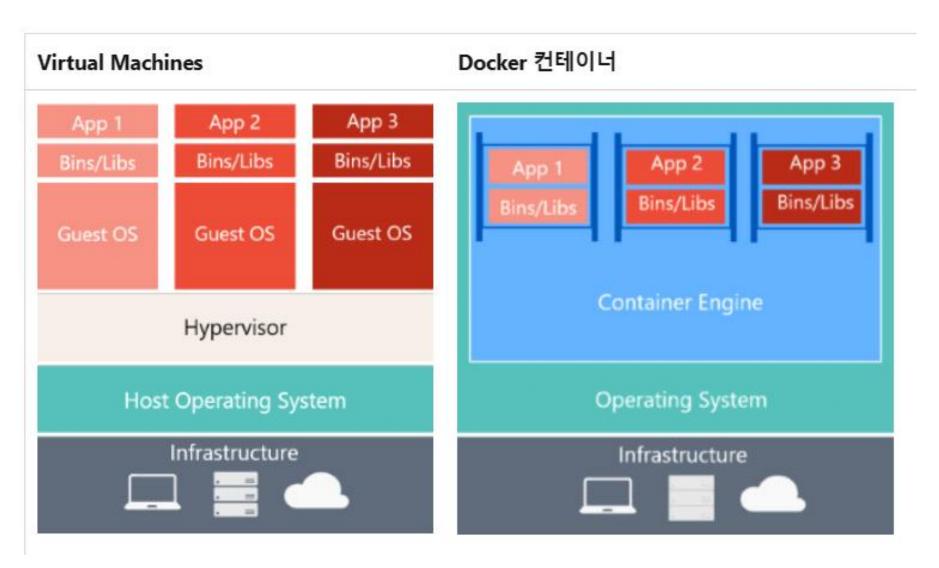
### Docker란?



- 1. 컨테이너 기반의 오픈소스 가상화 플랫폼
- 2. 리눅스 컨테이너에 리눅스 어플리케이션을 컨테이너로 프로세스 격리하여 실행 및 관리하는 프로젝트로 시작



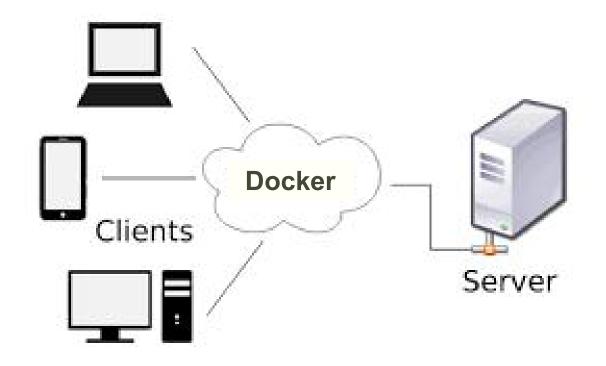
### Docker의 장점

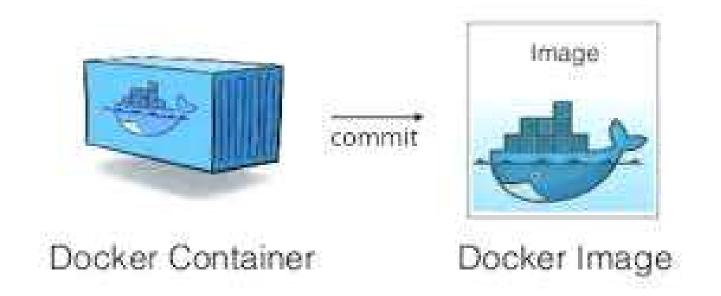


가상머신	도커
게스트 운영체제 사용을 위한 라이브 커널 포함 (큰 용량 배포)	커널을 공유해서 사용하기 때문에 컨 테이너에는 라이브러리 및 실행 파일 만 존재 (작은 용량 배포)
가상화된 공간이 하이퍼바이저를 거 치며 호스트에 비해 성능 손실 O	. 리눅스 자체 기능을 사용하여 프로세 스 단위의 격리 환경을 생성, 성능 손 실 X



### 도커의 장점





여러 개의 서비스를 1개의 서버에서 구동 용이

2. 대상 컨테이너 재현 용이



## 도커 사용량 추세

18 million +

developers

7 million +

applications

13 billion +

monthly image downloads



### 기업의 도커 이용

### See who uses Docker















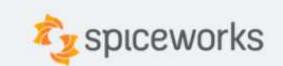




























### 개인의 도커 이용

### K-shield Jr 10기 취약점 진단 분반 프로젝트 <도커 사용 경험에 대한 설문조사> 폼

안녕하세요! 저희는 K-Shield Jr. 10기를 수강중인 학생들입니다⊜

현재 저희는 docker 취약점 진단 프로젝트를 진행하고 있습니다. 프로젝트 진행 중 docker 사용 경험에 대해 자료 수집이 필요한 부분이 있어 설문을 진행하려고 합니다.

설문대상은 도커 사용경험이 있는 IT 관련 종사자~경험자로, 개인, 팀 혹은 회사 프로젝트에서 도커를 사용하신 분들이라면 더욱 감사할 것 같습니다.爲

#### ✔K-Shield Jr.란?

향후 정보보호 분야 취업 시 현장 실무를 즉각 수행할 수 있는 사이버 보안 전문 주니어 인력 양성을 목표로 하는 프로그램입니다.

✓설문조사에서 제공해주신 개인정보(선택사항)는 프로젝트 종료 후 6개월 이내에 일괄 폐기될 예정입니다.

많은 참여 부탁드립니다!!!

[회사 프로젝트]

redis, kafka, MariaDB, MongoDB, ES 등을 구축할 때 이용. spring boot 및 flask 무중단 서비스 운영을 위해 사용. 서버의 운영체제 버전과 프로젝트의 호환성이 충돌하여 docker image를 통해 서버 배포

[회사 프로젝트] Deep learning 서비스를 위해 일정한 환경구축용 사용

[회사 프로젝트] 쿠버네티스에서 사용할 컨테이너 이미지 개발 [개인 프로젝트] CTF문제 제작 [팀 프로젝트] K Shield Jr 프로젝트 장고 서버 운영

개인 채굴 프로젝트

개인, 팀

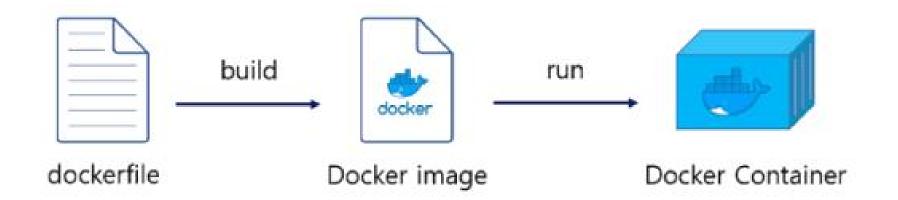
회사프로젝트 도커진단, 개인프로젝트 테스트 및 공부용도

[개인 프로젝트] 랩실에서 알파고 돌리기위해서 사용

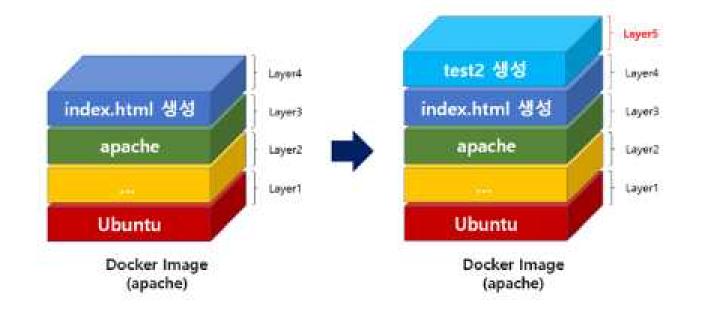


# 2. 악성 Docker 이미지 배포 및 Docker 취약성 사례

### 악성 Docker 이미지 배포



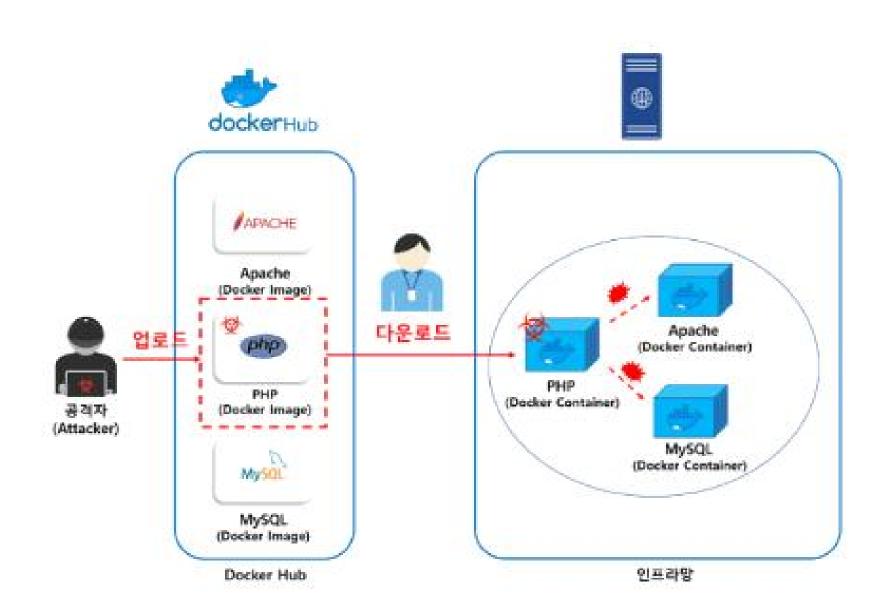
1. 도커 파일을 빌드하여 도커 이미지 생성



2. 기존 도커 이미지에 컨테이너에서 작업한 내역을 추가하여 새로운 도커 이미지 생성



## 악성 Docker 이미지 배포





### Docker 취약성 사례



Home > 전체기사

### 도커허브에서 1650개 이상의 악성 컨테이너 발견돼



도커허브의 높은 신뢰도 노린 공급망 공격...

요약: 도커 이미지들의 공공 저장소이자 가 악성 컨테이너가 발견됐다고 IT 외신 블리팅 암호화폐 채굴, 백도어, DNS 하이재킹, 웹시

도커 허브 컨테이너 이미지 50% 이상, 심각한 취약점 포함...잠재... 보안 전문가는 도커 허브(Docker Hub)에 호스팅 된 400만 개의 공개 도커 컨테이 너 이미지를 분석 한 결과 그 중 절반에 심각한 결함이 있음을 발견했다. 시큐리...



시스디그(Sysdig)가 25만 개의 이미지들을 검사하여 얻어낸 결과다. 이 컨테이너들을 의심 없이 받아로컬 시스템에 설치 후 사용하면 해당 시스템은 자동으로 암호화폐 채굴 기계가 되거나, 백도어 및 DNS 하이재킹 기능이 설치된 감시 기계가 된다.



# Docker 취약성 사례

### CVE Details

The arthering superty yalturninks of datasaurus

Lacks have the action of the lack of the l

Sign and state of the large of the Avenue S.

Stee CvT

THE RESIDENCE IN	

Section Colleges	control on the	Company.									Marie and a	Typeses in its	A STREET
16.4	Docker - Docker	Scourity V	Silverabilities										
travene v Ivendora Produkta	Cod State of American State  State Republic State Of State  Code Republic Described State  Code Republic Described State  Code Republic Described State  Cod State of Described State  Cod State of Described State  Cod State of State of State of State  Cod State of State of State of State  Cod State of State of State of State of State  Cod State of State of State of State of State  Cod State of State of State of State of State  Cod State of State of State of State of State  Cod State of	on the course y	B. B. B. J. S. S. W. B. Barris, Colombia y . D. W. B.	o p Sout Alby	1, 1, 91		out in						
On revealing to both	TVE ID	The second second	al Eroba a Makasanak yi Tembo	Probab Sido	Lodge Dide	See a	Date of Assess	-	Completely.		Carl	Library	***
emats a	Dec 2021-2020	256		S021 77 60	2022 0.25	200	How	Trems.	Modern and	Her topice.	30	Variation.	26.40
Administration of the	I a contemporarie with the form of a partner of the property of the contemporaries and the partner of the partn												
terch to the Security	2 130 200 21004	1722	Der Per		2002/04/29		TK W	Docal Security	100	400	7096	90.8	HON
Contract Contract  System orders of  Value of Replay (weeken)	the second and are also	Orași are an ex	TO DEL more des recombines all'allignes per communication from him of the specific consideration from consequent sections.										
e store tott beforensatt.	1 CHE 2020-20854	2	te to.	2029 11 20	2001 21 25	284	Heiron.	(Same)	- Dog	Margaret	- THE	3600	New
93.9	CAR WITH THE STORY	n in Audibra is	Coderand woods in 19 across	2000,000	es with a good	100 000	Strome encour	THE PERSON NAMED	harbs, torages	carry control bo	Seat to common a c	e gasasal az	10 m
Sade Possibles	4 25/2 2020 14300	- 273	Free Con-	2020-27 1	2023-09-1	23.6	Money	16.06	100	He species	No.34	Self #	200
e policiti e policiti Long arbitesi otaras sa Oligi i elemente L'Editalian de Alexandrian	tions of the state of the same	medical indep of the property of what had a not	publication of the state of the control of the cont	Citie Flore (reg deleta) Arrica don toirte (e	persent in this profession of the communities	agrande Normalista Narianno	of the Exitorically PS have exercised a leasing darker	o Salamania II La Patriciana La Represión	to the previous a sign of the train a sign sometimes	te parriedes in the e d'un sprofe de la e triery parte basis	estate prosp eriotes pado estate proces	es ar bac tant. Armijo de a e l Haji tin doard	ersey (a) in the Le mac to
Atlanta.	9460886689	4/4		2000 FG (CC)	200,0000	200	980H	11.1609	MV.	256000000000000000000000000000000000000	PMSH	293(4)	99.T0
Alberta of Contract Contractor Contractor	THIS ENGLISH WALL	all better year	n Heiferige in mie 7 fear Armen er janet fan Stadt Program in mar 7 fears Stadt	a the marks	and the same of	W 100 1	Called Services						
220	Name of the Copy	±1	Pepper	21+2-2	200200/	(S)	Home	belone.	1974	Service .	9 40	461.4	94.4
Sterior bings:	territory (Cont.)		OF UNIXAL CASES WERE NO.	erenia e	MARKET	e klatte	by as on an	100.64.5	costs (rus su)	media et as	ne e tetra e	chity, serie	fic the



### 프로젝트 진행 과정

Docker 진단 항목 수립

수동 진단

가동 스크립트 진단

Docker 취약점 상세보고서

KISA 클라우드 취약점 점검 가이드

> SK infosec 클라우드 보안가이드 Docker, Kubernetes

Doker 진단 가이드의 모든 항목에 대하여 수동 진단 후 '도커 취약점 수동점검 결과 리포트' 작성

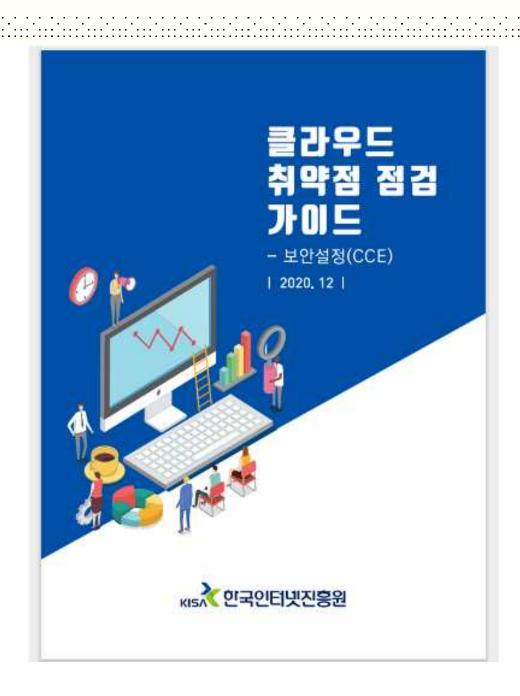
Docker 진단 가이드 '상' 항목에 대해 자동화 스크립트 작성

수동 진단 및 자동 진단 결과 보고서 작성

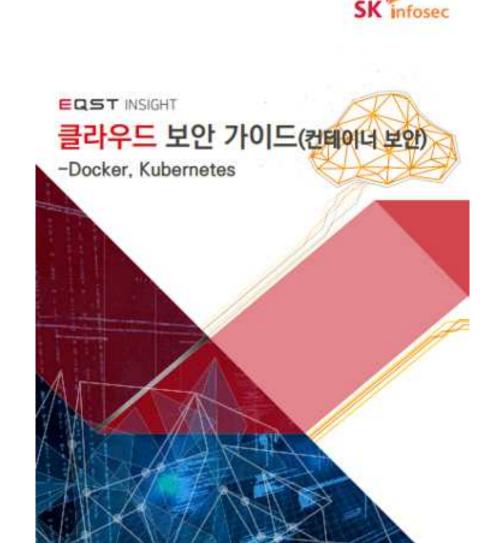


# 3. Docker 진단 항목 수립

### Docker 진단 항목 수립



KISA 클라우드 취약점 점검 가이드



SK infosec 클라우드 보안 가이드



# Docker 진단 항목 수립

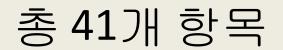
케이실도 루니어 10기 취직정진단분반 E-DI3

#### 목 차

진단코드	진단항목	취약도
D-01	도커화신 패치 적용	상
D-02	Docker daemon audit 설정	Nr.
D-03	/var/lib/docker audit 설정	상
D-04	/etc/docker audit 설정	삼
D-05	docker.service audit 설정	상
D-06	docker.socket audit 열정	상
D-07	/etc/default/docker audit 설정	삼
D-08	default bridge를 용한 컨테이너 간 네트워크 트래픽 제한	상
D-09	docker.service 소유권 설정	설
D-10	docker.service 파일 접근권한 설정	W.
D-11	docker,socket 소유권 설정	삼
D-12	docker.socket 파일 접근원한 설팅	Nr.
D-13	/etc/docker 디렉터리 소유권 설정	삼
D-14	/etc/docker 디렉터리 접근권한 설정	M
D-15	/var/run/docker.sock 파일 소유권 설정	삼
D-16	/var/run/docker.sock 접근 권한 설정	상
D-17	daemon.json 파일 소유권 설정	상
D-18	daemon.json 접근 권한 설정	상
D-19	/etc/default/docker 파일 소유권 설정	상
D-20	/etc/default/docker 접근 권한 설정	설

제이월드 주나에 10기 취약접진단본반 6-여 코

D-21	컨테이너에서 ssh 사용 금지	삼				
D-22	호스트 OS 주요 자원 접근 제어					
D-23	인증·권한 제어	삼				
D-24	SSL/TLS 적용	W				
D-25	컨테이너 권한 제어	8				
D-26	인증제이	**				
D-27	ssi/nis 적용	삼				
D-28	도커 그룹에 불필요한 사용자 제거	8				
D-29	legacy registry (v1) 비활성화	ō)				
D-30	추가 권한 획득으로부터 컨테이너 제한					
D-31	root가 아닌 user로 컨테이너 실행					
D-32	도커를 위한 컨텐츠 신뢰성 활성화					
D-33	컨테이너 SELinux 보안 옵션 설정					
D-34	컨테이너에서 privileged 포트 매핑 금지					
D-35	도커의 default bridge dockert) 사용 제한					
D-36	호스트의 user namespaces 공유제한	Ĝ.				
D-37	컨테이너 보안 정책	즇				
D-38	로그 관리					
D-39	Dockerfile Config					
D-40	이미지 취약정 및 구성 결합					
D-41	네트워크 제어	8				

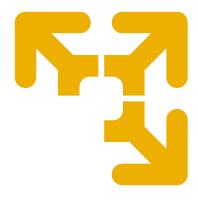




# 4. Docker 진단 환경 소개

### Docker 진단 환경

**VMW**are



**Ubuntu 18.04** 



docker 23.0.6



**MariaDB** 





# 5. 수동 진단

### 수동 진단

```
양호 : docker service 파일의 소유자 및 소유그룹이 rootroot인 경우
취약 : doctor.service 파일의 소유자 및 소유그룹이 rootiroot가 아닌 경우
ㅎ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음.
    agnentPath=/lib/systemd/system/docker,service
  eot@docker:~# is -1 /lib/systemd/system/docker.service
ru-r--r-- 1 root root 1730 Apr 14 10:32 /lib/systemd/system/docker.service
  eef@docker:"# stat —c #U:#6 /llb/systemd/system/decker.service
-> 소설자 및 소설그룹에 root-root 에므로 양호
DO-14. docker.service 파일 접근권한 실성
양호 : doctor.service 파일의 접근권한이 644 이하인 경우
취약 : docker service 박밀의 접근권한터 #44 호파인 경우

    * 미 파일은 시스템에 없을 수 있다. 그런 정우에는 권장 사항이 적용되지 않음.

   ootadacker:"# is -1 /lib/systemd/system/docker.service
na-r--r-- 1 root root 1730 Apr 14 10:32 /lib/systemd/system/docker.service
ootadacker:"# stat -c %a /lib/systemd/system/docker.service
-> docker service 파일의 정근원한미 644이므로 당호
DO-15. docker.socket 소유엔 설정
양호 : rlocker socket 파인의 소유자 및 소유그룹이 rootcroot인 정우
취막: docker socket 파일의 소유자 및 소유그룹이 roottroot가 마닌 정우
   oot@docker:"# systemoti show –p FragmentFath docker.socket
ragmentPaths/lib/systemd/system/docker.socket
oot@docker:"# is –1 /iib/systemd/system/docker.socket
n+r—r— 1 root root 195 nor 14 10:82 /iib/systemd/system/docker.socket
    otadocker: # stat -c 110:35 /lib/systemd/system/docker.cocket
-> docker socket 파인의 소용자 및 소유그룹이 rootiroot이므로 양호
DO-16. docker.socket 파벨 립근관한 설정
양호 : docker.socket 파일의 십근권한이 644 이하만 경우
취약 : docker eocket 파일의 접근권한미 644 초라인 경우
    tedocker: W systemoti show -p FragmentPath docker.socket
   ogmentPath=/llb/systemd/system/docker.socket
oot#docker:"A is ~1 /llb/systemd/system/docker.socket
no-r--r-- 1 root root 295 Apr 14 10:32 /llb/systemd/system/docker.socket
    reductions a stat -c sa /lib/systems/system/docker.socket
=> cocker.socket 파일의 월근권한이 644 이라이므로 양호
```

DO-13. docker.service 소유권 설정

DO-13. docker.service 소유권 설정 양호: docker.service 파일의 소유자 및 소유그룹이 root:root인 경우 취약: docker.service 파일의 소유자 및 소유그룹이 root:root가 아닌 경우 ※ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음.

root@docker:"# systemct1 show –p FragmentPath docker.service FragmentPath=/lib/systemd/system/docker.service root@docker:"# ls –1 /lib/systemd/system/docker.service –rw–r––r– 1 root root 1730 Apr 14 10:32 /lib/systemd/system/docker.service root@docker:"# stat –c %U:%G /lib/systemd/system/docker.service root:root

=> 소유자 및 소유그룹이 root:root 이므로 양호



### 수동 진단



K-Shield Jr 107

#### 도커 취약점 수동 점검 결과 리포트

#### 취약점 진단 E-01조

표재경

김서연

김효민

전동현

황유림

케이쉽드 주니어 107

취약점진단분반 E-01조

진단코드	D-09	참고	kisa DO-13 / sk 2.1					
진단항목명	docker.service 소유권 설정	취약도	kisa 상 / sk 하					
진단기준								
양호	docker.service 파일의 소유자 및 소유그룹이 root:root인 경우							
취약	약 docker.service 파일의 소유자 및 소유그룹이 root:root가 아닌 경우							
진단방법								

파일 경로 확인 : systemctl show -p FragmentPath docker.service 소유권 확인 : Is -l /lib/systemd/system/docker.service stat -c %U:%G /lib/systemd/system/docker.service

#### 진단결과

oot@docker:″# systemctl show -p FragmentPath docker.service 'ragmentPath=/lib/systemd/system/docker.service root@docker:″# 1s -1 /lib/systemd/system/docker.service ro⊢----- i root root 1730 Apr 14 10:32 /lib/systemd/system/docker.service 'oot@docker:″# stat -c %U:%G /lib/systemd/system/docker.service

#### 비고

※ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음.

진단코드	D-10	참고	kisa DO-14 / sk 2.1						
진단항목명	docker.service 파일 접근권한 설정	취약도	kisa 상 / sk 하						
	진단기준								
양호	docker.service 파일의 접근	권한이 64	4 이하인 경우						
취약	취약 docker.service 파일의 접근 권한이 644 초과인 경우								
	진단방법								

파일 경로 확인: systemctl show –p FragmentPath docker.service 접근권한 확인: Is –l /lib/systemd/system/docker.service stat –c %a/lib/systemd/system/docker.service

#### 진단결과

root@docker:″# 1s -1 /1ib/systemd/system/docker.service -rw-r--r-- 1 root root 1730 Apr 14 10:32 /11b/systemd/system/docker.service root@docker:″# stat -c %a /1ib/systemd/system/docker.service

#### 비고

※ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음.



# 6. 자동스크립트 진단

## 자동 스크립트 진단

구분	진단모드	진단 항목	취약되
	D-01	도위의신 패치 책용	427
	D-01	(kiea(DO-01), slq(5;3))	0
	D-02	Docker deemon eudit 설명	45
	D-92	(hise(DO-08), sld(2.2))	(2)
	D-03	/var/lib/docker audit 質問	44
	D-00	(Rise(DC-04), sk(2.2))	0
	D-04	/etc/docker audit 個階	42
	5.04	(bisa(DO-05), sio(2.2))	=
	D-05	docker service audit 설정	18
	7.00	(hisa(DO-06), sit(2.3))	10
	D-08	doctor societ audit 설명	-9
	7.00	(Maa(DO-07), els(2.2))	-
	D-07	/etc/default/docker audit 결정	42
	2.00	(hisa(DO-08), slo(2,2))	0
	D-08	deCault bridge를 통한 전테이너 간 네트워크 트래픽 계한	8
	5.00	(htsa(DO-09), sto(1.8))	9.
	D-08	docker.service 소유권 설정	7
	- "	(idsa(DO-19); sic(2.1))	-
	D-10	docker service 파일 접근권한 설정	15
		(Riea(DO-14), slo(2.1))	
	D-11	docker.socket 소유권 설정	4
	F0.55	(hisa(D0-16), sln(3.1))	-
	D-12	docker socket 파일 접근원한 설정	당
		(kise(DO-18), elc(2.1))	-
	D-13	/etc/docker 디렉터리 소유권 설정	74
	2.00	(hisa(DO-17), sk(2.1))	6
	D-14	/etc/docker 디펙터리 접근원한 설정	4
	E933	(hisa(DO-18), sin(3.1))	
	D-18	/var/run/docker.sock 확립 소유권 설정	18
		GGes(DO-19), slc(2.1))	. 4.
	D-16	/ver/rum/docker.sock 접근 원한 설정	생
	10000	(itisa(DO-20), sto[2,1])	5
	D-17	deemonjeon 파일 소유원 설정	12
		(hisa(DO-31), sk(3.1))	. "
	D-18	daemon jeon 접근 원한 설명	42.
	30,000	(Rise(DO-22), sk(2.1))	
	D-19	/etc/default/docker 파일 소유권 설정	4
	(200T)	(Risa(DO-23); slo(2.1))	33
	D-20	/etc/default/docker 접근 권한 설정	12
		(hisa(DO-24), sld(2.1))	14.
	D-31	런테이너에서 sob 사용 금의	*
	EXCESS	(kiss(DO-28), sk(1:5))	750
	D-22	호스트 06 주요 자원 청군 제어	18

	(els(1.1))	
D-23	인중-권환 제어	AT.
D-13	(els(1.2))	Ö
D-24	SSL/TLS 적용	상
2.14	(eld(1.3))	
D-25	컨테이너 권한 제어	상
D-20	(ek(1.7))	3
D-26	인중제어	44
D-20	( els(4.1))	3
D-27	SSL/TLS 적용	*
10-27	(els(4.2))	0



### 자동 스크립트 진단

#### 리눅스 쉘 스크립트

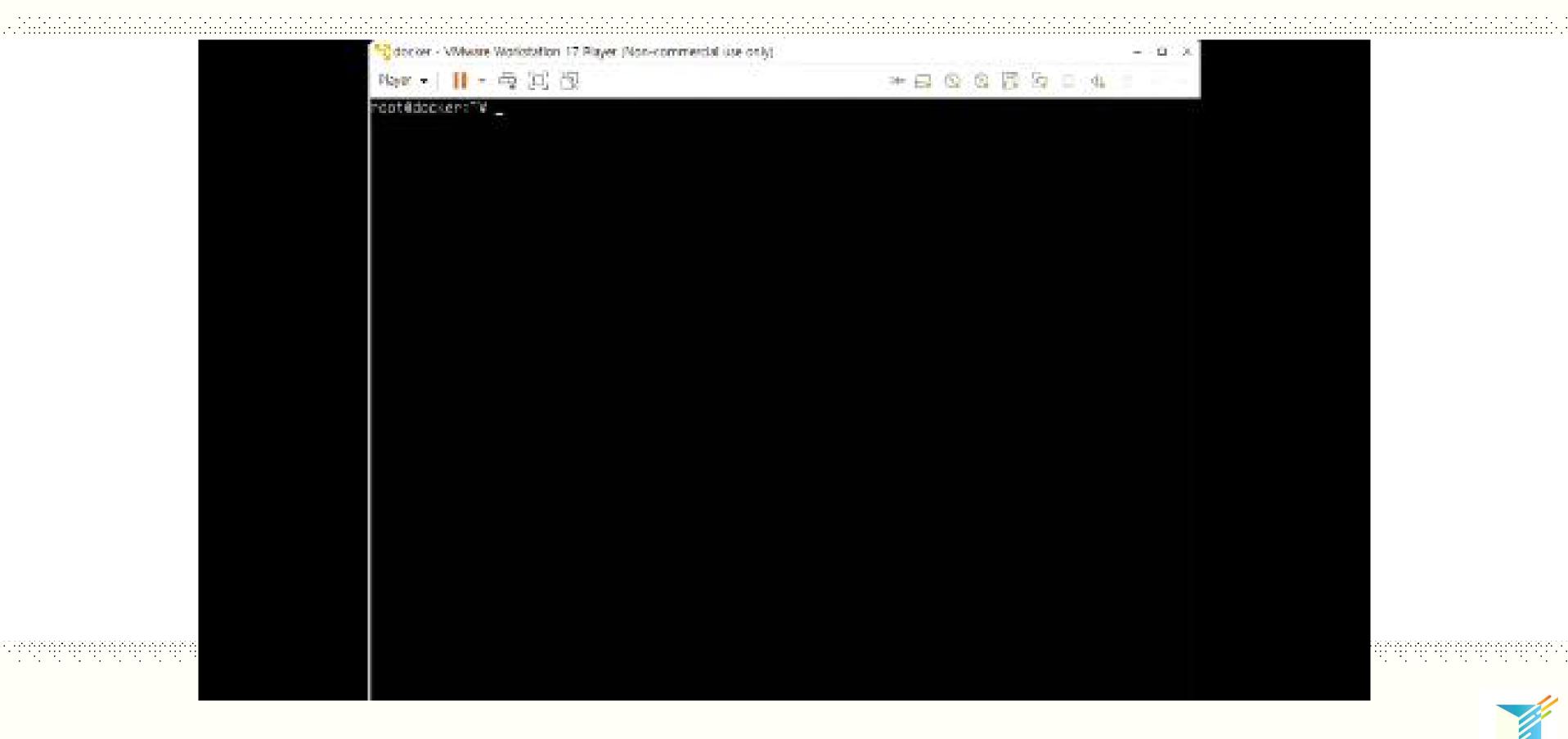
```
'[ DO-16 ]: Cehck"
'==========[ DO-16 START ]" >> $RESULT_FILE 2>&1
      " >> $RESULT_FILE 2>&1
DOCKER_SOCKET_FILE=$(systemctl show -p FragmentPath docker.socket | awk -F= '{print $2}')
if [ -e "SDOCKER_SOCKET_FILE" ]; then
        ls -1 $0
        permission_val=
        owner_perm_val= echo "$
group_perm_val= echo "$
        other_perm_val=`echo "$
  then
                 echo "Result: Good" >> $RESULT_FILE 2>&1
        else
                 echo "Result: Vulnerable" >> $RESULT_FILE 2>&1
        fi
else
        echo "docker.socket file not found." >> $RESULT_FILE 2>&1
echo "Result: Review" >> $RESULT_FILE 2>&1
                 =========[ D0-16 END ]" >> SRESULT_FILE 2>&1
```

#### 쉘 스크립트 진단 결과 파일

```
======[ DO-16 START ]
Result: Good
======[ DO-16 END ]
======[ DO-17 START ]
drwxr–xr–x 2 root root 4096 May 5 21:17 /etc/docker
Result: Good
======[ DO-17 END ]
 :======[ DO-18 START ]
drwxr–xr–x 2 root root 4096 May  5 21:17 /etc/docker
Result: Good
======[ DO-18 END ]
======[ DO-19 START ]
srw–rw––– 1 root docker 0 May 14 14:24 /var/run/docker.sock
Result: Good
 ======[ DO-19 END ]
======[ DO-20 START ]
srw–rw––– 1 root docker O May 14 14:24 /var/run/docker.sock
Result: Good
```



## 자동 스크립트 진단 실행 영상





# 7. Docker 취약점 상세 보고서

# Docker 취약점 상세 보고서

Docker 취약점 점검 상세 보고서

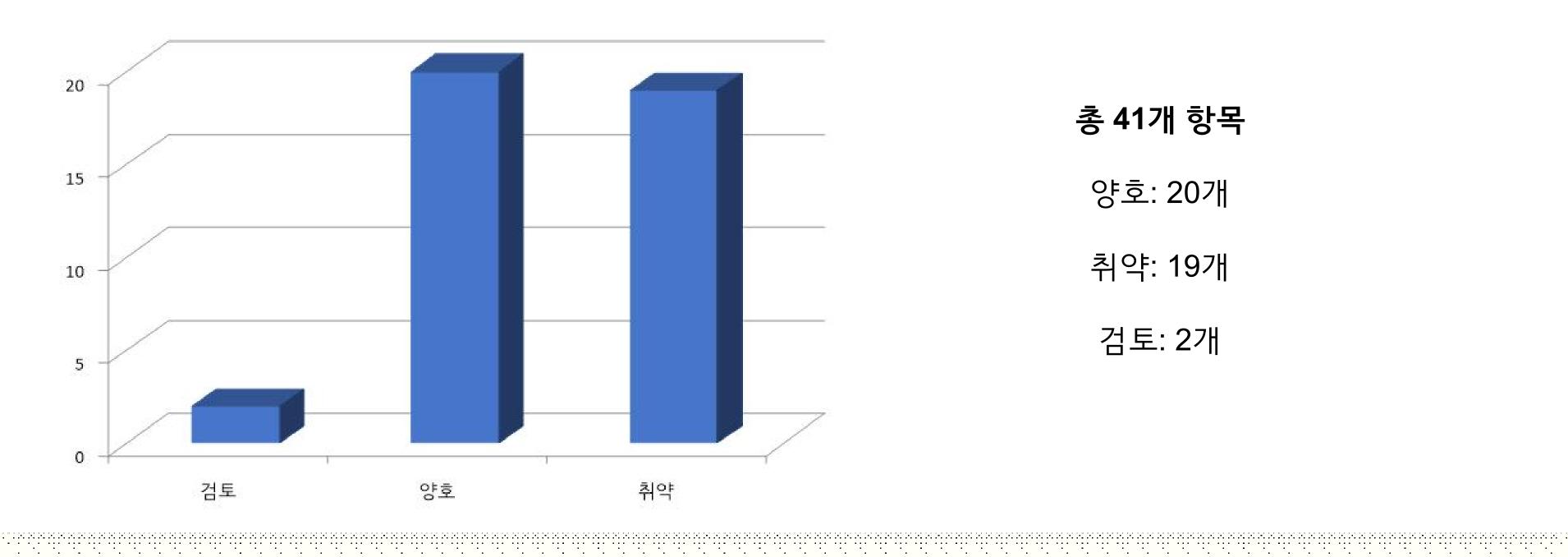
2023. 05. 17

	(in)			
-	I had about			
		**		
	2224		83	M040
	<b>EMHT 用打力器</b>	41	***	
	Deber premor aut; IFE	-90	**	
OET.	national season with the	7	-	
064.	I I I I I I I I I I I I I I I I I I I	- 60	11.0	
	Some stone and \$25 Some stone and \$25	41	0.4	
(WT	Anny Street Street Carlot Call	41	7.5	
197.	ANTI-PROPERTY AND SA	4	**	
00t	#de.0 500pc를 통한 1943년 (1 세트시프 드리트 위한:	*		
000	監判 建甲甲烷基 改作 養別	.14	***	
rp.	Building parties II R S (18)	4	- 44	
	Accompany 418 Octob 419	10	8.5	
	Actorises a CAS SS	. 10		
	Access access THE TOTAL WIT	10	- RE	
	Anti-Market 口間経過 小学者 装装	w	8.0	
TH.	envisides FIRFIT SIZ SIT MS	- 66	-	
	- Dealth and Allert Annual - Still Server		120	
680	Angelian policy of man 阿斯·沙拉·雷拉		0.6	
un.	Newhorkson son tigt ## ##		100	
010		40	0.0	
	demonstra BC 34/ Will	44	-	
		4	-	
	Microsoft Colored Total Colored Colore	- 10	0.1	
	PPER14回日 山上 4月 331	- 10	-	
00%	Why sproop Apr		9.0	
004	直出區 (2) 今至 中市 性計 特別	-65	-	
#h	전에 생활 되다.	10	ná	
	(10.735. 発養	4.	1112	
110	CHEST ST. WA	1	0.5	
0.36	건축에서:	-27	3.8	
231	46.715.71B	++	-	
da.	토리 그래의 문학들은 시르다 점은		100	
	He0040	LT.	1	
mit	1994年 中国の大大打工管官所	16.	9.1	
-	AT AN ELECTRIC HART MA BRITAIN	-	-	
mm.	artis	2	9.5	
IIII.	SAFE THE SAME STOP IN STREET STORY STORY	A	0.0	
114	左州軍 神界 中外岛 沙泉州 衛州市	4		
_	heaptical anniti	-		
	(100mm SEE 100 AC 100)		25	
211	9960 CTL WILK!	-6	me	
	10.1 pc. 4764-00044			
			1	
M/A	PROPERTY AND ADDRESS OF THE PROPERTY AND ADDRESS OF T	7	100	
1128	VAR etca terra service His Michigania			
0.77	B(1.5)	+	11-0	
me.	第八月日 upon regrangueses 亜鉛環性 princ (b) John DD-121, (a)(1-0)	-81	44	
0.00	GMMH 공간 중설	4	ing	
4.25	part ap	-	1110	
940	#1 84 http://	*	0.7	
0010	Dedorfile Carlos		1	
211	HALTIF	*		
Gal	보다지 취하철 및 구성 경찰 2011-70	3	10.00	1



### 진단 결과

### 각 항목별 진단 결과



### 총 41개 항목

양호: 20개

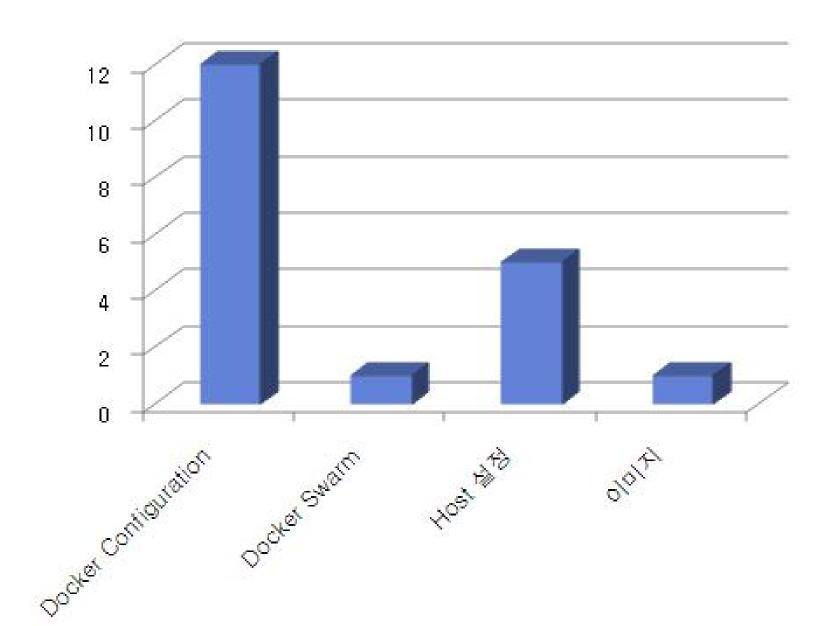
취약: 19개

검토: 2개



## 취약 항목





총 19개 항목

Docker Configuration: 12개

Docker Swarm: 1개

Host 설정: 5개

이미지: 1개



# 취약 항목 보호 대책

Docker Configuration	Docker Swarm	Host 설정	이미지
도커 컨테이너 각 설정 파일 내부 설정을 알맞게 변경한 후 서비스 재실행 필요	SSL/TLS 적용 필요	docker 감사 파일 설정 추가 필요	dockerfile 내 ADD 명령어 대신 COPY 명령어 사용 필요

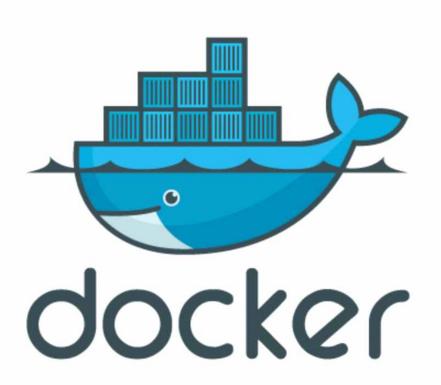


# 8. 기대효과

## DOCKER 취약점 진단 필요성

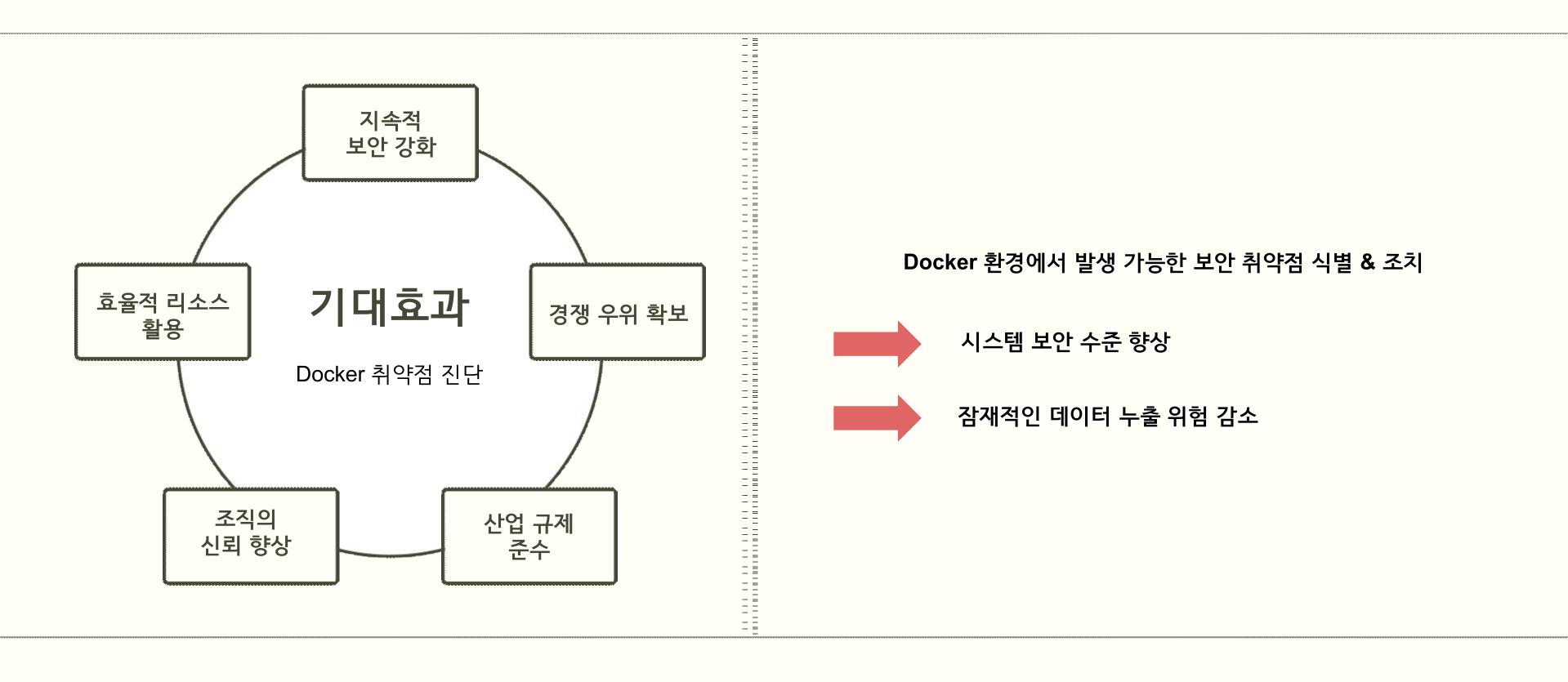
#### **DOCKER**

- . 현대 애플리케이션의 개발과 배포는 컨테이너화 기술인 Docker의 사용으로 큰 변화 O
- . Docker 환경에서의 보안 취약점은 여전히 중요한 문제 존재
- . 전체적인 취약점 식별과 보안요소 체크
  - ⇒ 애플리케이션 및 시스템의 안전성 보장





### Docker 취약점 진단 기대효과





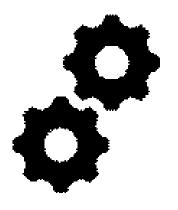
지속적 보안 강화



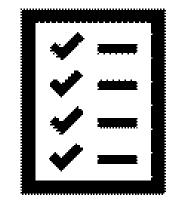
조직의 신뢰 강화 & 경쟁우위 확보

산업 규제 준수



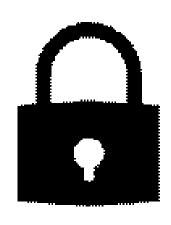








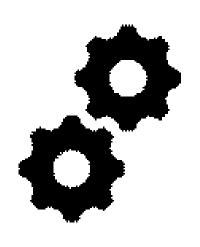
### 지속적 보안 강화



- . 단기적 사용이 아닌 지속적 보안 강화를 위한 도구로 활용
- . 새로운 취약점 발견 & 보안 요구사항 변경 시
  - ⇒ 스크립트 업데이트를 통한 최신 보안 취약점을 식별 및 대응 가능
- 조직의 보안 위협에 대응하고 시스템의 지속적인 보안 강화 목표 달성 가능



### 효율적 리소스 활용



- . 대량의 컨테이너 및 이미지를 효율적으로 분석 가능 (Docker 취약점 진단 스크립트는 자동화된 방식으로 작동)
- 보안 전문가 및 개발자의 시간과 노력을 절약하고, 업무 효율성을 향상 가능
- . 스크립트의 결과 및 보안 취약점 보고서를 통해 리소스 할당 및 우선순위 설정에 도움



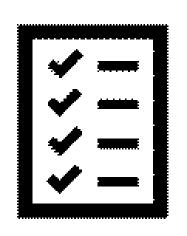
### 조직의 신뢰 강화 & 경쟁 우위 확보



- . 조직의 보안인식을 강조하고 고객, 파트너, 규제 기관 등과의 신뢰 강화에 기여
- 보안에 대한 책임감을 보여주고 고객 정보와 기업 자산을 안전하게 보호 가능
- . 조직이 경쟁 환경에서 우위를 점하는 데 기여
  - ⇒ 보안 취약점으로인한 시스템 다운타임 & 데이터 유출 시시
  - ⇒ 심각한 비용과 이미지 손상
- . 스크립트를 사용하여 취약점을 사전에 발견하고 대응
  - ⇒ 조직의 안정성과 신뢰성을 강조하며 고객과 파트너들에게 더 큰 신뢰를 줄 수 있음



### 산업 규제 준수



- . 다양한 산업 분야에서 보안 규제 및 규정 준수는 필수적
- . Docker 취약점 진단 스크립트를 사용하여 조직은 규제 요구 사항 확인 가능

  ⇒ 보안 관련 감사 및 인증 절차를 통과 가능
- 지속적 보안 취약점진단을 통해 조직의 비즈니스 확장과 고객의 신뢰 유지에 기여



# 9. 인사이트

### **INSIGHT**

- . 클라우드 보안 취약점 진단 가이드에서 취약도 '상' 기준의 항목만 체크
  - → 향후 진단 스크립트를 발전시켜 나머지 '중', '하' 항목에 대해서도 적용 필요
- . 다양한 조건에서의 취약점 진단 여부 확인 미흡
  - → 정책적인 요소를 통한 접근, 컨테이너 내부의 악성 이미지 환경에서의 취약점 진단 부족
- . Docker 취약점 진단 스크립트의 지속적 개선과 혁신 필요
  - → 보안 커뮤니케이션을 통한 스크립트 지속 개선과 취약점 식별의 중요성 이해
  - → 새로운 보안 조치 및 정책 개발에 대한 인사이트 제공을 통한 보안 역량 강화 기대



# 감사합니다