국가보안기술연구소

사이버 훈련의 이해

사이버안전훈련센터
2020. 7. 15.
강정민

CONTENTS

1

훈련의 중요성

훈련 [訓鍊] 가르칠 훈, 단련할 련

“ 재주나 기예 따위를 배우거나 익히기 위해 **되풀이**하여 연습함 ”

“ 일정한 목표나 기준에 도달할 수 있도록 정신적으로나 육체적으로 실천시키는 **실제적** 교육 활동 ”

다양한 분야의 훈련

재난, 질병, 군사위협 등에 신속한 대응을 위함

(COVID-19) 국민의 생명을 살린 훈련

2019.04.23

2019.11.17 중국의 첫번째 사례(추정)

2019.12.17 질병관리본부 전염병 전문가 24명 훈련 완료

2020.01.04 재난대응 알고리즘 실전 적용 준비완료

2020.01.07 중국의 코로나 사태 인식

2020.01.09 실제상황 적용 테스트

2020.01.27 국내 4명 확진, 펜데믹에 대비

2020.03.11 WHO 팬데믹 선언

(COVID-19) 훈련 경험으로 빠른 대응 성공

CSTEC 사이버안전훈련센터

"

중국에 여행을 다녀온 한국인 가족이 숨을 쉬기 힘들어하는

원인 모를 증상을 호소하고 관련 의료진에게도 급속히 퍼졌다

- 2019.12.17 질병관리본부 훈련 시나리오-

"

WORLD NEWS MARCH 30, 2020 / 1:15 PM / 3 MONTHS AGO

South Korea's emergency exercise in December facilitated coronavirus testing, containment

Hyonhee Shin 4 MIN READ

SEOUL (Reuters) - A South Korean tabletop exercise on emergency responses to a fictional mysterious outbreak led directly to tools the country deployed less than a month later to manage the arrival and spread of the coronavirus, one of the experts involved said.

실전과 유사한 훈련(시나리오)의 필요성

NSR

I 2 I

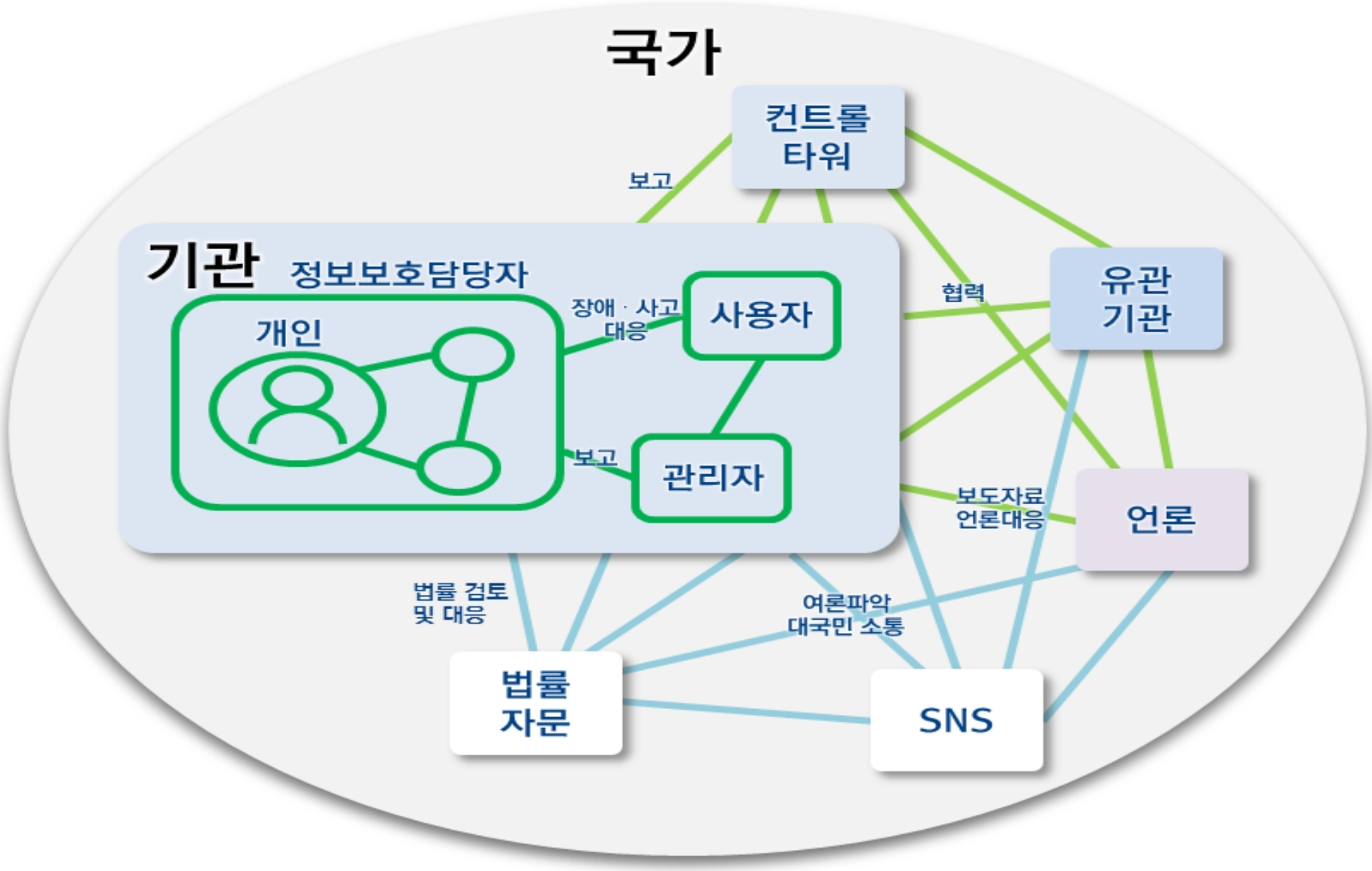
사이버 훈련

전략 2. 사이버공격 대응역량 고도화

“ 대규모 공격 대비태세 강화 ”

- 국가 사이버안보 전략 (2019. 4.) -

사이버 훈련 범위

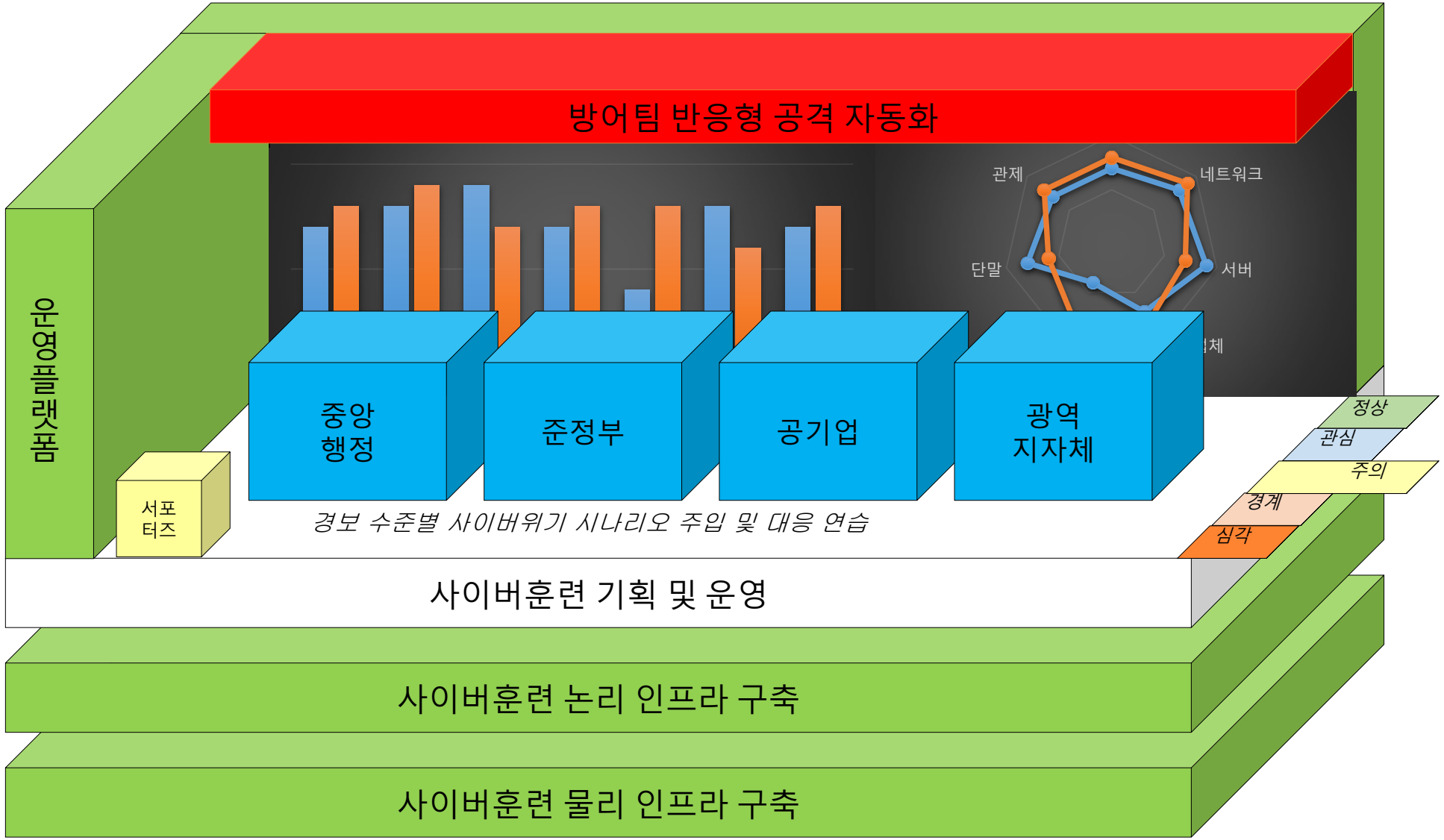

국가
컨트롤 타워
보고
기관
정보보호담당자
개인
장애 · 사고 대응
사용자
보고
관리자
협력
유관 기관
보도자료 언론대응
언론
법률 검토 및 대응
여론파악 대국민 소통
법률 자문
SNS

사이버 훈련 시스템(1/3)

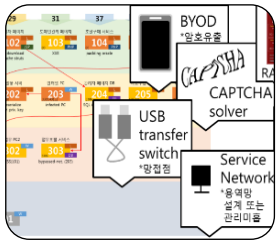
훈련시스템 = **Red 시스템 (공격)** + **Green 시스템 (운영, 관리)** + **Blue 시스템 (방어)**

참가팀	팀 별 역할
화이트팀 WT (White Team)	대회 운영 및 데이터 확보 ① 사이버 공격・방어 데이터 확보 및 분석 ② 훈련 콘텐츠 개선 방법론 개발
레드팀 RT (Red Team)	블루팀에 대한 사이버 공격 담당 ① 블루팀에 대한 방어 역량 검증을 위한 사이버공격 감행 ② 최신 훈련용 사이버 공격 관련 기술적 데이터 확보
그린팀 GT (Green Team)	시스템 설계・구축 및 관리 ① 대회 운영을 위한 시스템 설계・구축 ② 원활한 대회를 위한 시스템 운영 및 관리
블루팀 BT (Blue Team)	사이버방어 훈련 및 역량평가 ① 실전 훈련을 통한 사이버 방어 대응능력 확보 ② 콘테스트 방식의 개인 및 팀 역량 평가 * 역량 평가 결과를 활용할 수 있는 정책 필요
옐로팀 YT (Yellow Team)	대회 운영 지원 및 방어 팀 지원 ① 서포터즈 중 일부가 블루 팀의 일원으로 참여하여 실제 상황 지원 ② 블루 팀에 대한 사이버 방어 대응 현환 모니터링 및 지원

사이버 훈련 시스템(2/3)


방어팀 반응형 공격 자동화
관제
네트워크
단말
서버
체
운영플랫폼
중앙
행정
준정부
공기업
광역
지자체
서포
터즈
정상
관심
주의
경계
심각
경보 수준별 사이버위기 시나리오 주입 및 대응 연습
사이버훈련 기획 및 운영
사이버훈련 논리 인프라 구축
사이버훈련 물리 인프라 구축

사이버 훈련 시스템(3/3)



훈련 콘텐츠

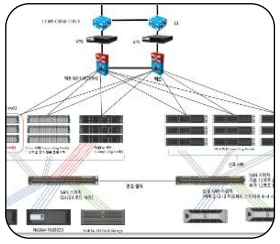
- 시나리오, 블루팀 미션, 레드팀 스케쥴, 평가방법
- 법, 미디어, 전략, 점수화, 규칙, 인력 운영

운영 플랫폼

- 포털(VM접속 콘솔, 점수 확인 등), 가용성 확인, 소통채널
- 훈련 현황 시각화, 뉴스사이트, 모니터링(감사) 등

가상 인프라

- 가상 HOST 배포, POST SCRIPTING, 계정 관리
- 가상 네트워크 구성(IPS, 방화벽, 라우터, 스위치 등)



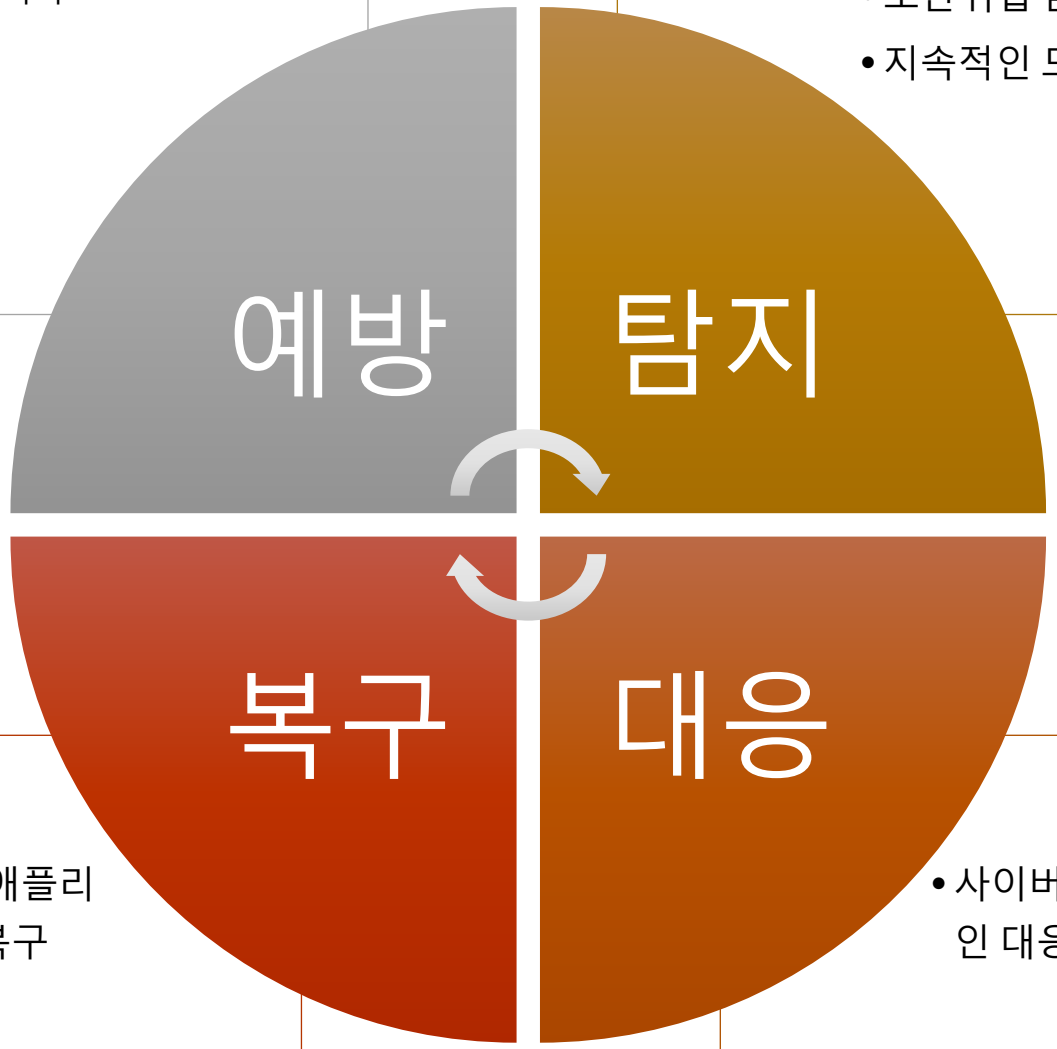
물리 인프라

- 망 운영 계획(VPN 사용여부 등)
- 서버, 네트워크, 계정 관리

사이버 훈련과 복원력 (1/3)

- 리스크 및 취약성 파악
- 개선 로드맵 수립
- **사이버훈련**

선제적 예방



- 보안위협 탐지 및 분석
- 지속적인 모니터링

- 중요 데이터, 애플리케이션 신속 복구
- 정상상태 유지

- 사이버 공격에 효과적인 대응 및 조치

사이버 훈련과 복원력 (2/3)

사이버 복원력 프레임워크(Cyber Resilience Engineering Framework, MITRE, 2011) 및 평가

예1) 침해 당한 시스템의 정상동작 까지 걸리는 시간(정상입증)으로 이해, 제약, 지속, 재구성 항목을 평가

Practices(세부기술)

평가항목(Practices)
최적 대응
분석 모니터링
보호 조정
기만
다양화
동적 배포
동적 흐름 표현
비지속성
권한제한
재정렬
중첩
분할
정상입증
예측불허

Objective(목표)

평가항목(Objectives)
이해(Understand)
준비(Prepare)
예방(Prevent)
제약(Constrain)
지속(Continue)
재구성(Reconstitute)
변형(Transform)
재설계(Re-Architect)

Goal(목적)

평가항목(Goals)
예측(Anticipate, Plan)
지속(Withstand, absorb)
회복(Recover)
진화(Evolve, adapt)

- by MITRE -

사이버 훈련과 복원력 (3/3)

사이버 복원력 프레임워크(Cyber Resilience Engineering Framework, MITRE, 2011) 및 평가

예2) 네트워크 패킷에서 공격자의 IP식별(분석 모니터링) 성공 시 이해, 준비, 제약, 재구성 항목 평가

Practices(세부기술)

평가항목(Practices)
최적 대응
분석 모니터링
보호 조정
기만
다양화
동적 배포
동적 흐름 표현
비지속성
권한제한
재정렬
중첩
분할
정상입증
예측불허

Objective(목표)

평가항목(Objectives)
이해(Understand)
준비(Prepare)
예방(Prevent)
제약(Constrain)
지속(Continue)
재구성(Reconstitute)
변형(Transform)
재설계(Re-Architect)

Goal(목적)

평가항목(Goals)
예측(Anticipate, Plan)
지속(Withstand, absorb)
회복(Recover)
진화(Evolve, adapt)

- by MITRE -

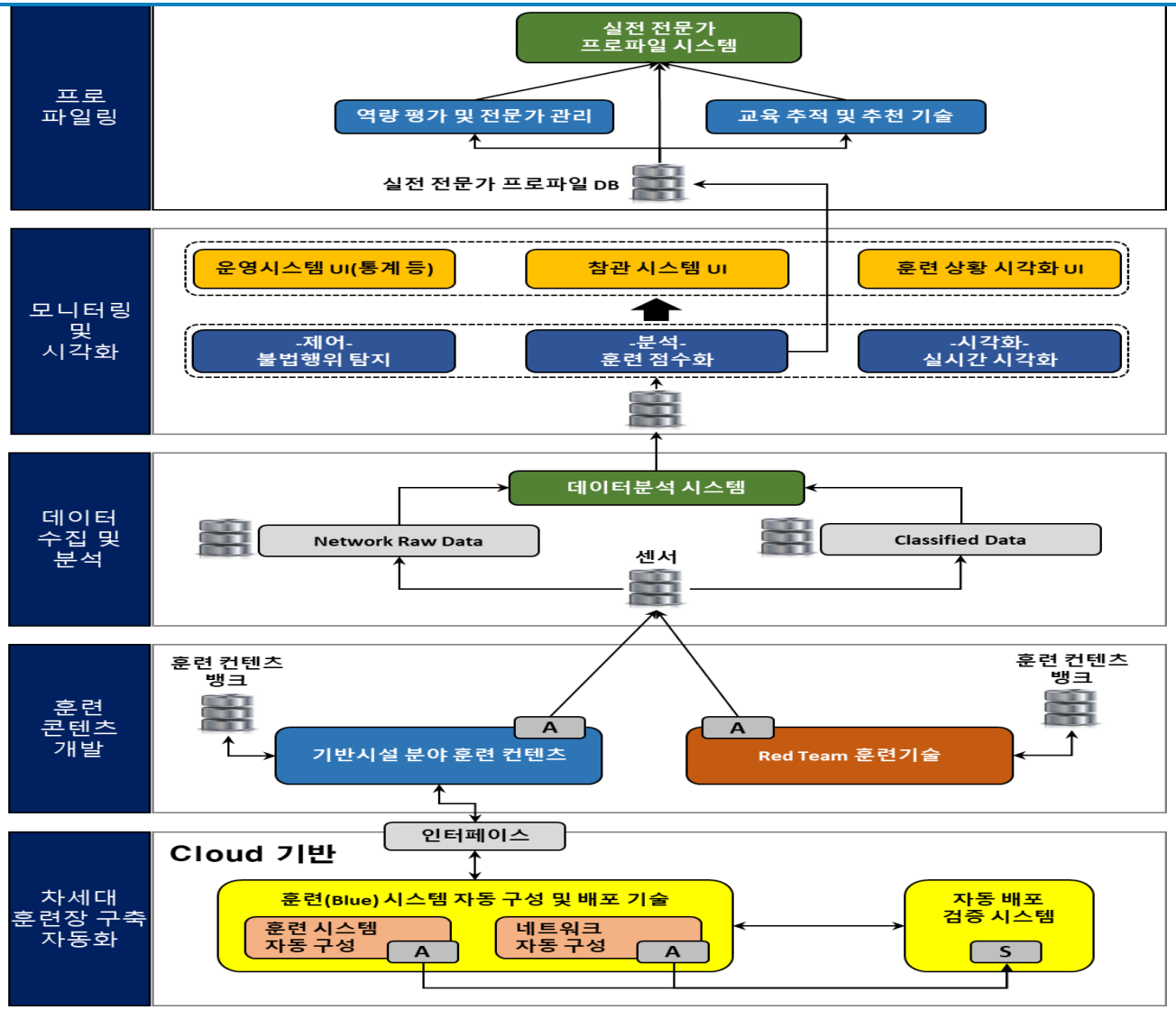
I 3 I

사이버훈련 기술

사이버 훈련 세대 구분

	Red 시스템 (공격)	Green 시스템 (운영, 관리)	Blue 시스템 (방어)
1 세대	• 사람중심의 단일공격 시스템	• 운영, 관리, 평가시스템 • 진행상황 모니터링	• IT 인터넷망(PC, Web, SW) 업무망 • OT 정수, LNG 등 기반시설
한 계		• 단순 평가를 위한 채점 위주의 시스템	• 확장성 부족 • 소규모 훈련 지원
2 세대	• AI, 자동화를 통한 복합적인 콘텐츠 생성 • 병렬적, 동시다발적인 공격 시나리오 수행	• 훈련 데이터 수집 (빅데이터) • 빅데이터를 통한 훈련 결과 분석 • 시각화된 분석결과 제공	• IT와 OT의 복합적인 훈련 환경구축 • 모듈화된 설계로 기반시설 추가기능 지원 (확장성)

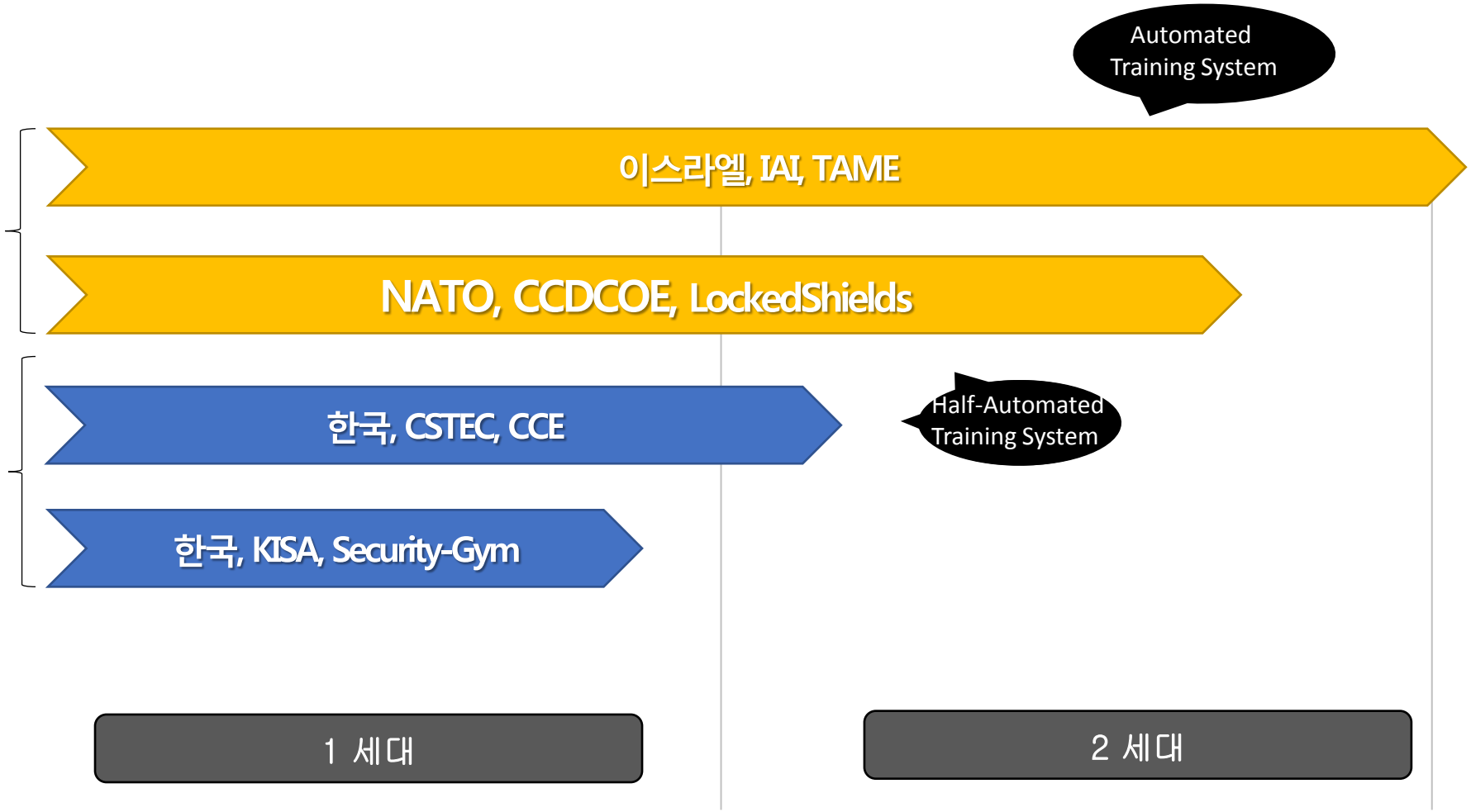
차세대 훈련 기술



차세대 훈련시스템(2세대)은 대규모 참가자가 IT·OT 융복합 시스템 대상

공방 동시훈련을 수행하기 위해 첨단 기술을 적용한 유연하고 확장 가능한 시스템

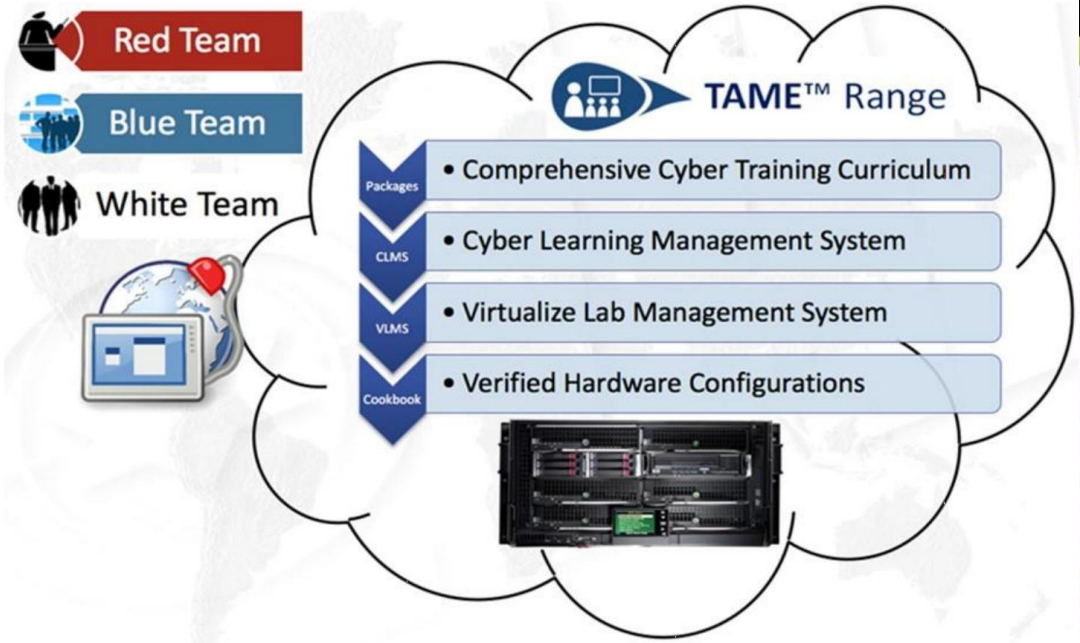
국내외 훈련 기술 수준



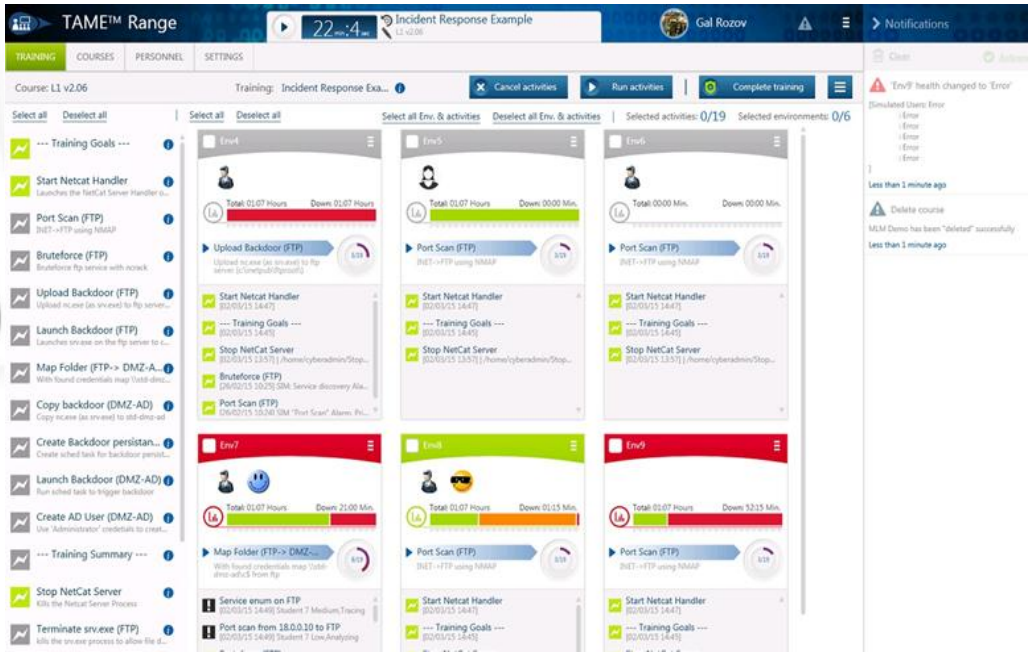
훈련장 구축 유연성, 콘텐츠 구성 자동화 등을 고려

TAME by IAI(ISRAEL)

- ❖ 자체 클라우드 하드웨어 환경 구축
- ❖ 가상 훈련환경을 통해 다수의 훈련을 동시다발적으로 진행
- ❖ 사이버 교육 관리 시스템으로 수준별 훈련 진행
- ❖ 특정 위협을 포함한 100개 이상의 시나리오
- ❖ 자동화된 공격시나리오를 통해 최소 인력으로 훈련 가능

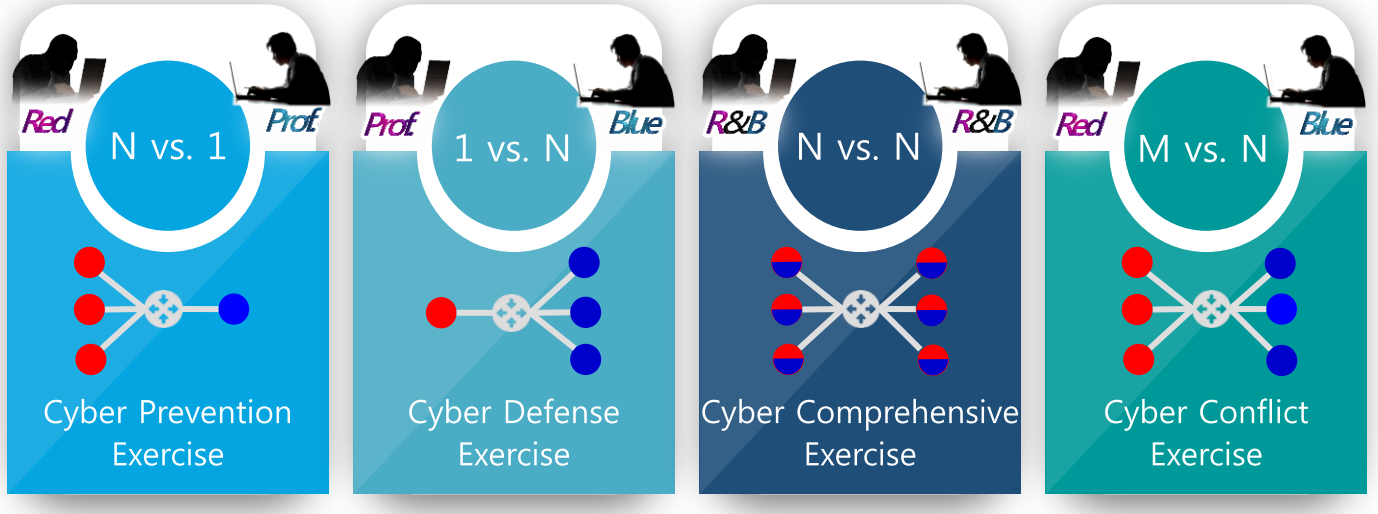


TAME훈련장 구조



훈련 포탈

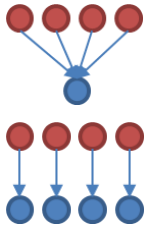
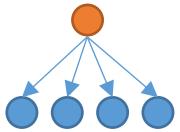
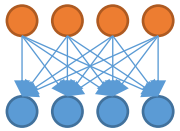
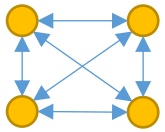
사이버 훈련 모델



- N vs. 1
  - CTF(Capture The Flag)
- 1 vs. N
  - LockedShields, Cyber Conflict Exercise (2019)
- N vs. N
  - Defcon
- M vs. N
  - Cyber Conflict Exercise (2017-2018)

사이버 훈련 모델

CSTEC 사이버안전훈련센터

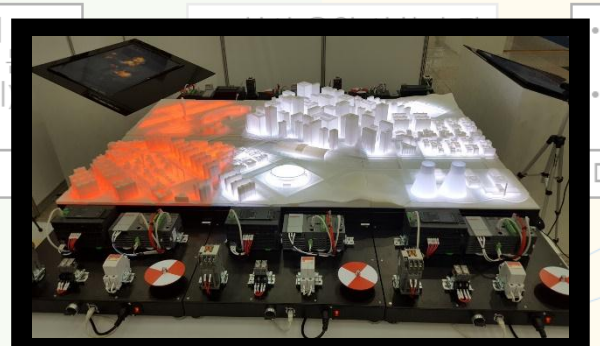
	 CTF Capture The Flag	 Locked Shields	 Cyber Conflict Exercise	 Defcon
인력양성	공격 및 방어 가장 많이 알려진 방식	방어중심 실전과 유사한 환경	공격 및 방어 역할에 따른 전문가 양성	공격 및 방어 공격과 방어를 동시에
확장성 더 많은 참가팀	용이함 미션 당 1개 VM	어려움 방어팀 제공 VM x 방어팀 수	어려움 방어팀 제공 VM x 방어팀 수	어려움 방어팀 제공 VM x 방어팀 수
공정성유지	용이함 동일한 환경 제공 가능	용이함 레드팀의 가급적 공정한 공격	어려움 레드팀의 선택	어려움 레드팀의 선택
미션구성	용이함 공격, 방어 모두 가능	용이함 방어미션 중심	어려움 복합적인 공격 및 방어 미션	용이함 주어진 조건이 동일
운영난이도	**용이함** 힌트로 미션풀이 속도 조절	용이함 준비된 공격 스케쥴	**어려움** 공격팀의 미션 풀이 속도가 중요	용이함 주어진 조건이 동일
스토리구성	용이함	실제	관점 다양 레드팀도 참가자	게임과 유사
점수화	CTF CTF는 미션풀이 결과를 인증하는 가장 쉬운 접근방법 중 하나임	종합적 레드팀 공격 증빙(스크린샷), SLA, 상황보고, 법/미디어 대응, 포렌식 챌린지 등	**종합적** CTF(공격팀), SLA, 패치검증서버, 상황보고, 미디어대응 등	

주어진 목표와 활용 가능한 자원을 고려한 모델 선택이 필요

NSR

훈련 보조시스템

티켓팅 시스템(트러블슈팅)



기반시설모사시스템(훈련효과)

가용성 점수화 시스템

포털 시스템

훈련망 (가상 네트워크: DMZ, EXT, INT, CTL)

- 방어팀 전용 미션 뉴스 게시(운영팀)
- 상황파악 후 댓글로 정보공유(방어팀)

미디어(뉴스)

다수 IP를 이용한 훈련트래픽 관리

훈련트래픽 관리

- 일반 7개팀
- 일반 초정 1개팀

방어팀

공격팀 미션

공격팀 미션풀이에 필요한 힌트 제공

용역 사무실

- 점수확인
- 미션확인(공격팀)
- 메모,상황보고(방어팀)

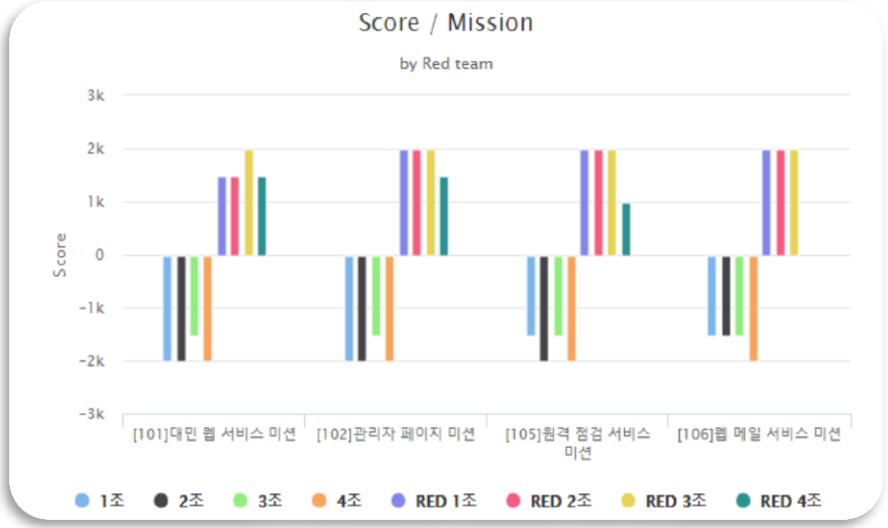
CCE포털시스템

- 대회 운영에 필요한 파일 공유
- 팀원간 파일 공유

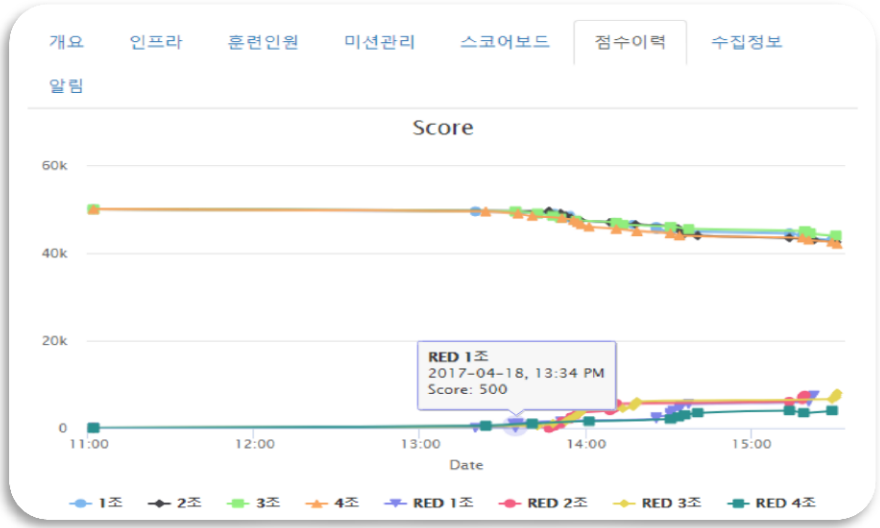
공유폴더

훈련 보조시스템: 훈련 포털(1/2)

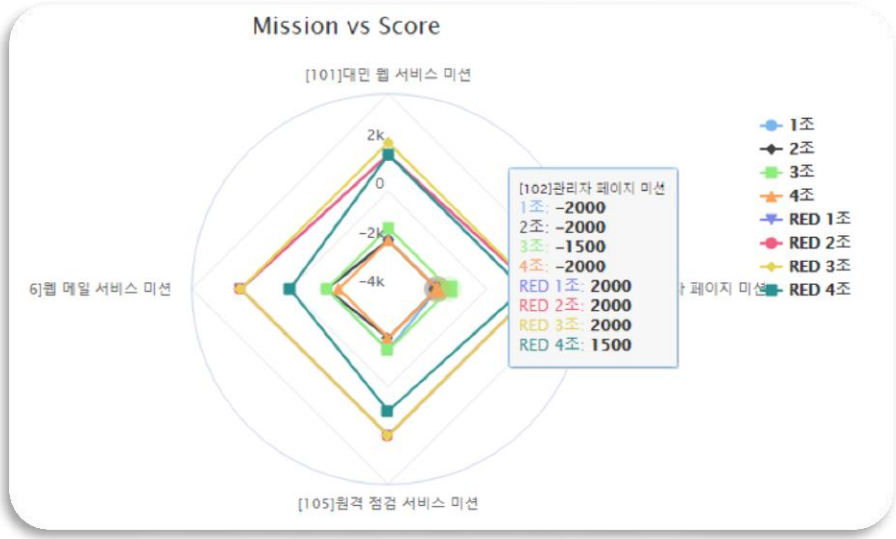
CCE 포털 메인 화면



팀별 미션 풀이 상황 정보

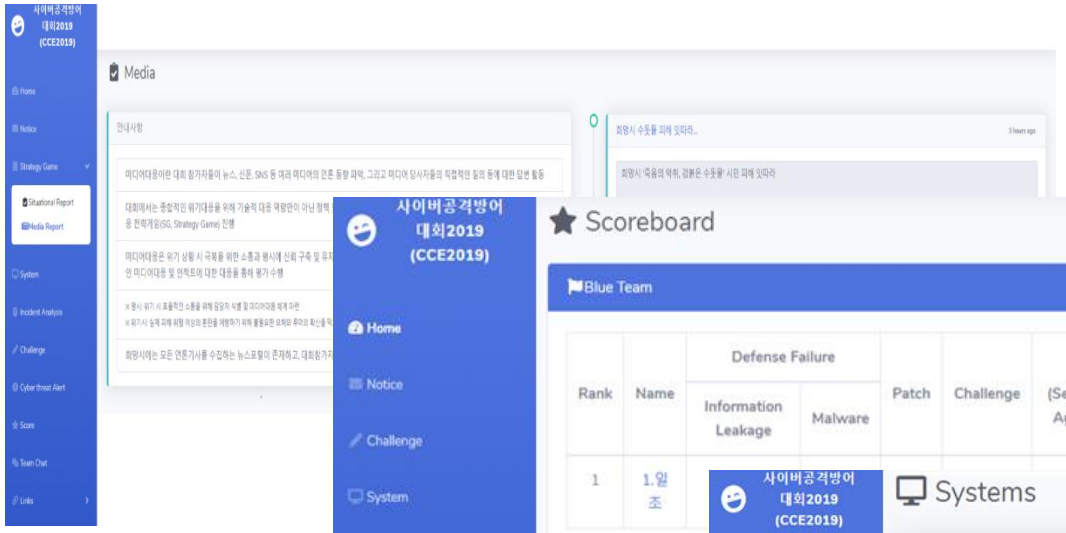


훈련 조별 스코어 추이

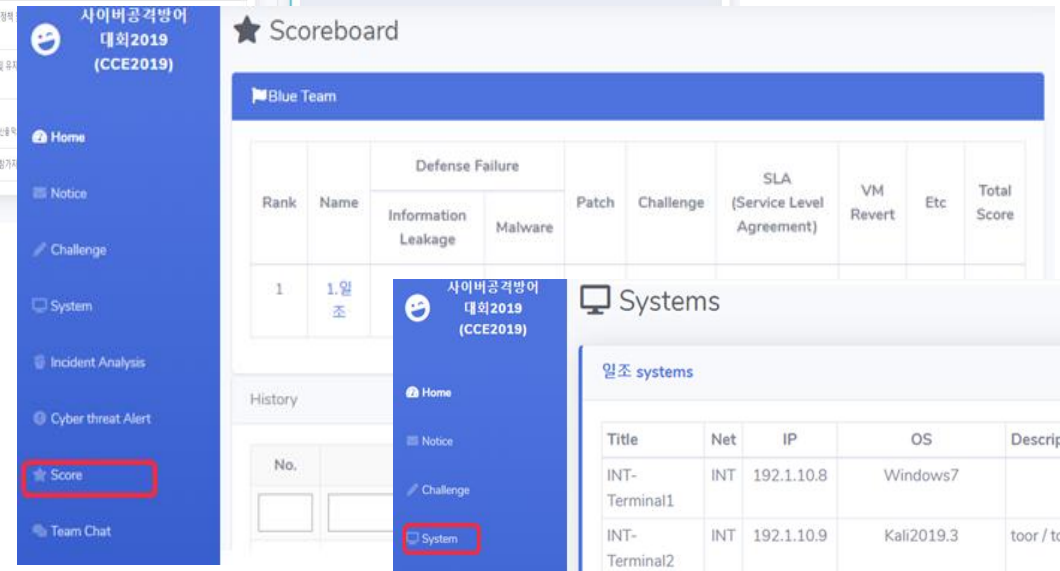


미션 유형 별 강점, 약점 분석 정보

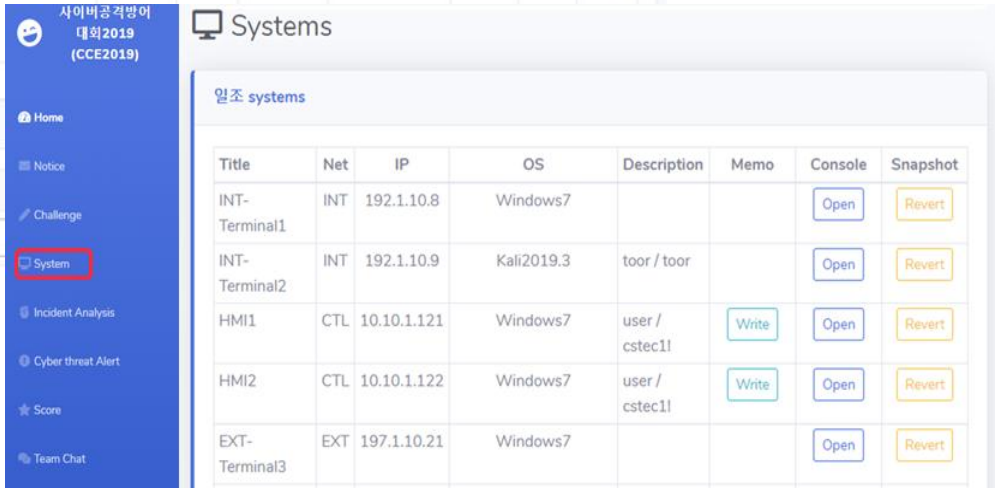
훈련 보조시스템: 훈련 포털(2/2)



미디어 대응

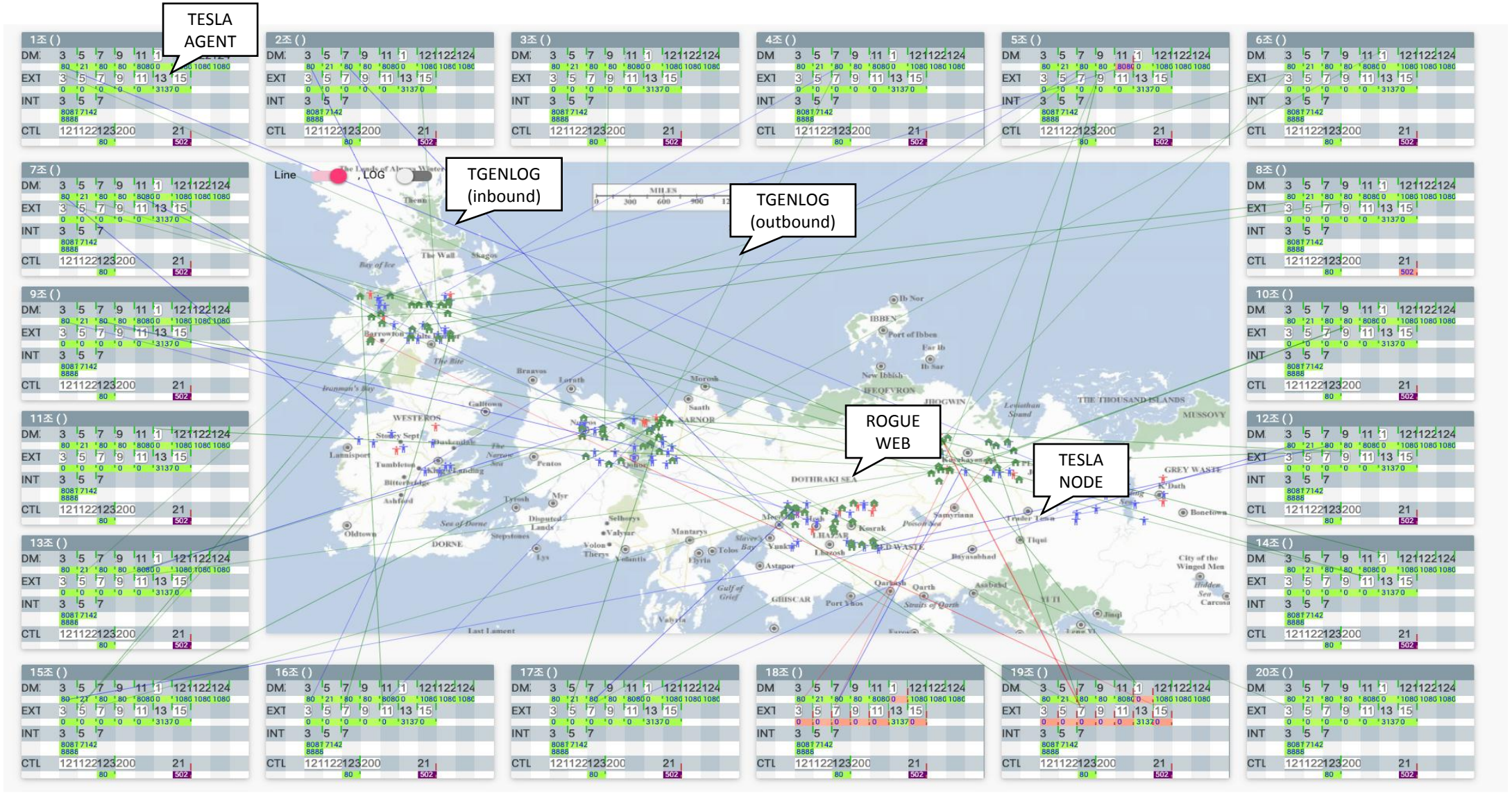


점수판



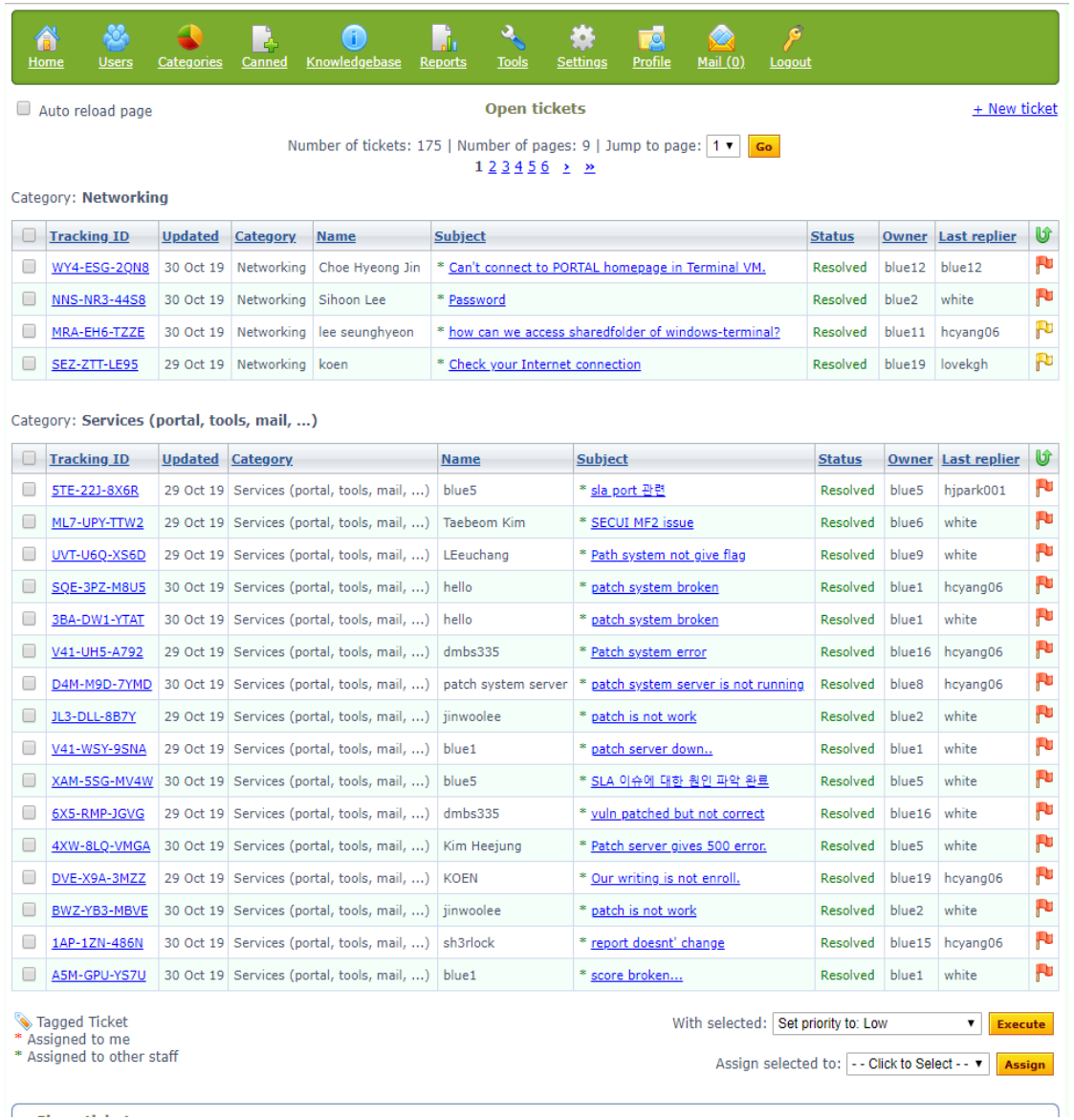
방어팀 시스템 접속

훈련 보조시스템: 가용성 점수화 시스템



- 방어팀에게 제공된 시스템/서비스/기능이 정상적으로 운영 중인지를 확인
- SLA(Service Level Agreement)

훈련 보조시스템: 티켓팅 시스템



Home | Users | Categories | Canned | Knowledgebase | Reports | Tools | Settings | Profile | Mail (0) | Logout

Auto reload page

Open tickets

+ New ticket

Number of tickets: 175 | Number of pages: 9 | Jump to page: 1 Go

1 2 3 4 5 6 › »

Category: **Networking**

Tracking ID	Updated	Category	Name	Subject	Status	Owner	Last replier
WY4-ESG-2QN8	30 Oct 19	Networking	Choe Hyeong Jin	* Can't connect to PORTAL homepage in Terminal VM.	Resolved	blue12	blue12
NNS-NR3-44S8	30 Oct 19	Networking	Sihoon Lee	* Password	Resolved	blue2	white
MRA-EH6-TZZE	30 Oct 19	Networking	lee seunghyeon	* how can we access sharedfolder of windows-terminal?	Resolved	blue11	hcyang06
SEZ-ZTT-LE95	29 Oct 19	Networking	koen	* Check your Internet connection	Resolved	blue19	lovekgh

Category: **Services (portal, tools, mail, ...)**

Tracking ID	Updated	Category	Name	Subject	Status	Owner	Last replier
5TE-22J-8X6R	29 Oct 19	Services (portal, tools, mail, ...)	blue5	* sla port 관련	Resolved	blue5	hjpark001
ML7-UPY-TTW2	29 Oct 19	Services (portal, tools, mail, ...)	Taebeom Kim	* SECUI MF2 issue	Resolved	blue6	white
UVT-U6Q-XS6D	29 Oct 19	Services (portal, tools, mail, ...)	LEeuchang	* Path system not give flag	Resolved	blue9	white
SQE-3PZ-M8U5	30 Oct 19	Services (portal, tools, mail, ...)	hello	* patch system broken	Resolved	blue1	hcyang06
3BA-DW1-YTAT	30 Oct 19	Services (portal, tools, mail, ...)	hello	* patch system broken	Resolved	blue1	white
V41-UH5-A792	29 Oct 19	Services (portal, tools, mail, ...)	dmbs335	* Patch system error	Resolved	blue16	hcyang06
D4M-M9D-7YMD	30 Oct 19	Services (portal, tools, mail, ...)	patch system server	* patch system server is not running	Resolved	blue8	hcyang06
JL3-DLL-8B7Y	29 Oct 19	Services (portal, tools, mail, ...)	jinwoolee	* patch is not work	Resolved	blue2	white
V41-WSY-9SNA	29 Oct 19	Services (portal, tools, mail, ...)	blue1	* patch server down..	Resolved	blue1	white
XAM-5SG-MV4W	30 Oct 19	Services (portal, tools, mail, ...)	blue5	* SLA 이슈에 대한 원인 파악 완료	Resolved	blue5	white
6X5-RMP-JGVG	29 Oct 19	Services (portal, tools, mail, ...)	dmbs335	* vuln patched but not correct	Resolved	blue16	white
4XW-8LQ-VMGA	30 Oct 19	Services (portal, tools, mail, ...)	Kim Heejung	* Patch server gives 500 error.	Resolved	blue5	white
DVE-X9A-3MZZ	29 Oct 19	Services (portal, tools, mail, ...)	KOEN	* Our writing is not enroll.	Resolved	blue19	hcyang06
BWZ-YB3-MBVE	30 Oct 19	Services (portal, tools, mail, ...)	jinwoolee	* patch is not work	Resolved	blue2	white
1AP-1ZN-486N	30 Oct 19	Services (portal, tools, mail, ...)	sh3rlock	* report doesnt' change	Resolved	blue15	hcyang06
A5M-GPU-YS7U	30 Oct 19	Services (portal, tools, mail, ...)	blue1	* score broken...	Resolved	blue1	white

Tagged Ticket
* Assigned to me
* Assigned to other staff

With selected: Set priority to: Low Execute

Assign selected to: - - Click to Select - - Assign

- 참가자와 운영자 간 소통 채널이 되는 시스템
- 카테고리 별로 담당자가 답변 가능
- 티켓팅 시스템: 이메일, 채팅과 같이 다양한 소통채널 준비

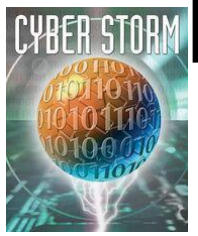
Ⅰ 4 Ⅰ

국내외 사이버훈련

국외 사이버 훈련

NSA/CSS Cyber Defense Exercise (USA NSA) 2001

네트워크 구축, 확보, 방어를 목표로 함



Cyber Storm (USA DHS) 2006

전략적 의사결정 및 절차, 기관 간 정보 공유

Cyber Europe (ENISA) 2010

비즈니스 연속성, 위기 관리 상황 대처 능력 평가

Crossed Swords (NATO CCDCOE) 2016

IT시스템의 취약점 파악을 목표로 함

2004 Cyber Drill (APCERT)

악성코드 중심 (악성코드로 인한 DDoS)

2008 Cyber Coalition (NATO)

의사결정 과정, 기술 및 운영절차 협업 등을 평가

2010 Locked Shields (NATO CCDCOE)

시나리오, 전략게임, 미디어, 법, 기술, 소통 등이 어우러진 훈련

2017 EU CYBRID (EU)

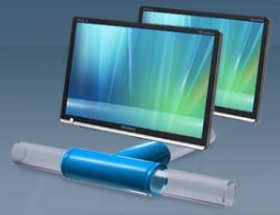
EU 국방장관들이 참여하는 사이버 방어 전략 도상훈련

Locked Shields by NATO CCDCOE

CSTEC 사이버안전훈련센터

NATO CCDCOE 회원국의 민·관·군 보안전문가들이 참여하여
사이버 위협에 대한 대응 준비태세를 점검하고
서로의 실력을 겨루는 국제 사이버 방어훈련

사이버 공격에 대한 기술적 대응 외에도
언론·법·전략, 포렌직 대응 등의 능력을 종합적으로 평가



NATO CCDCOE에서 주관하여
2012년 이후 매년 에스토니아 탈린에서 개최
(모든 방어팀은 VPN을 통해 온라인 참여)

NSR

Locked Shields by NATO CCDCOE

CSTEC 사이버안전훈련센터

Exercise	Number of Blue Teams (BTs)	Nations represented in Blue Teams	BT size cap	VMs per team	Persons involved
Baltic Cyber Shield 2010	6	3 + NATO	10		< 100
Locked Shields 2012	9	9 + NATO	10	~25	250 +
Locked Shields 2013	10	9 + NATO	12	34	~ 250
Locked Shields 2014	12	14 + NATO	16	50	300
Locked Shields 2015	15	16 + NATO	16	~75	400
Locked Shields 2016	20	19 + NATO	16	~75	550 +
Locked Shields 2017	20	19 + NATO	∞	120	~ 800
Locked Shields 2018	22	20+NATO+EU	∞	150	1000
Locked Shields 2019	23	21+NATO+EU	∞	150	1200

Locked Shields by NATO CCDCOE

기반시설모사시스템 by NSR

- ❖ 기반시설 모사시스템 6종(전력, 항공, 정수, 교통, 철도, 원자력)
- ❖ 17년부터 매년 LockedShields에 국가보안기술연구소 참여(BT, RT)

사이버공격방어대회(CCE)

CSTEC 사이버안전훈련센터

2016

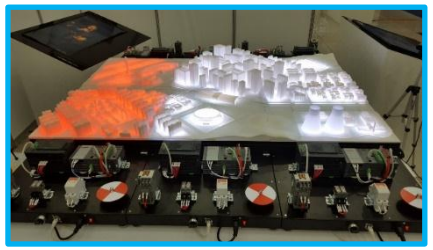
사이버실전종합훈련

공격 4팀(BoB), 방어 8팀(공공)

공격-방어 훈련 포맷 도입

대전
사이버안전훈련센터

2017



제1회 사이버공격방어대회

- 공격 10팀(에스토니아 초청), 방어 16팀
- 민간-공공 합동 대회로 변경
- 기반시설 모사시스템 개발 및 적용
- 총 상금 6,000만원

서울
The K 호텔

2018

제2회 사이버공격방어대회

- 공격 10팀(체코 초청), 방어 16팀
- 종합적 방어(상황보고, 미디어대응) 도입
- 물리 보안 챌린지 이벤트
- 총 상금 7,000만원

제주
메종글래드 호텔

2019

제3회 사이버공격방어대회

- 공격팀(운영진), 방어 20팀(체코 초청)
- 예선전 223개팀 참가 (18년 대비 약 2배)
- 방어 중심 대회 훈련 포맷, 종합적 사이버 대응 역량 평가(기술요소 외 사고분석, 전략게임 등)
- 총 상금 5,500만원, 국정원장님 상장

부산
벡스코

NSR

I 5 I

2020 사이버공격방어대회

NSR

2020 사이버공격방어대회

CSTEC 사이버안전훈련센터

목표

국가 재난 시 사이버 시스템을 정상으로 복원할 수 있는
사이버 복원 역량 점검(부제: 사이버 복원력 강화)

예선

9월 26(토), 09:00~24:00
참가팀 : **제한 없음,** 본선 진출 : 30개팀(**팀별 4인** 이내)

본선

10월 29일(목)	09:00~21:00	대회 본선 1일차	사이버 위기 단계별 사이버 공격 대응 및 복원 역량 점검
10월 30일(금)	09:00~12:00	대회 본선 2일차	
	13:30~14:00	온라인 시상식	-
	14:00~16:30	패널토의	대회 수상자 결과 브리핑, 실시간 Q&A - 발표 : 대회 수상자(1위~3위) - 참가 : 대회 참가자 및 일반 참가자
	16:30~17:00	경품 추첨	-

주최/주관: 국가정보원/국가보안기술연구소

NSR

국가보안기술연구소

감사합니다