보안 운영환경 및 신기술 파악을 위한

공무 국외출장 시행 결과(보고)

'19. 9.

보안정보전략실

정 보 보 안 팀

작성자 : 직원 박상훈(☎8374)

목 차

1. 목　　적

□ 최신 정보보안 위협 및 해킹기술 변화 파악

□ 사이버위협 대응 기술 및 최신 트렌드 습득

□ 신재생에너지 원격운전 현장 방문을 통한 신재생 보안기술 습득

2. 출장 개요

□ 출 장 지 : 미국(라스베가스, 샌프란시스코)

□ 출장기간 : '19. 8. 5. ~ 14. (8박 10일, 출국 : 8월5일, 입국 : 8월14일)

□ 출 장 자 : 정보보안팀 팀장 김재성, 직원 박상훈

□ 주요일정

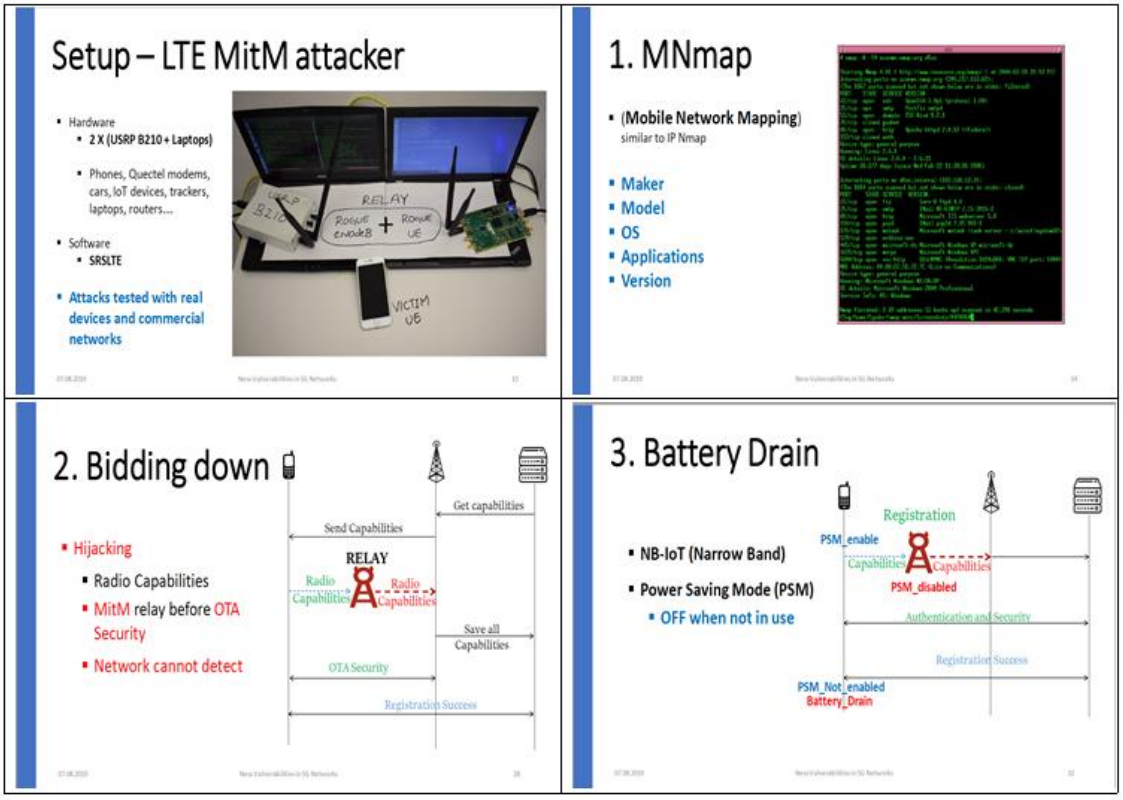
구 분	주요 내용	비 고
8/5(월)	출국 및 라스베가스 도착	인천 → 라스베가스
8/6(화)	Black Hat 기술전시회 참관 - 사이버위협 인텔리전스(CTI), 엔드포인트 보안 플랫폼(EPP) 등	Black Hat
8/7(수) ~8(목)	Black Hat Conference 세션1 참가 - 지능형 위협탐지, 사고 분석 및 취약점 대응 기술 Black Hat Conference 세션2 참가 - 산업제어시스템 공격/방어, 현대적 DDoS 공격/방어 기술	Black Hat
8/9(금)~ 8/10(토)	DEFCON 27 사이버경진대회 참관, 컨퍼런스 참가 - IoT, 기반시설 제어시스템 등 해킹기술 참관 및 토론 DEFCON 27 운영기관 미팅	DEFCON
8/11(일)	이 동	라스베가스 → 샌프란시스코
8/12(월)	연료전지 시스템 적용 사이버보안기술 확인 - 블룸에너지社 연료전지 엔지니어 실무회의	블룸에너지(주)
8/13(화) ~14(수)	귀국 및 인천 도착	샌프란시스코 → 인천

3. 출장 수행 내용

가. Black Hat 2019 기술 전시회 및 컨퍼런스

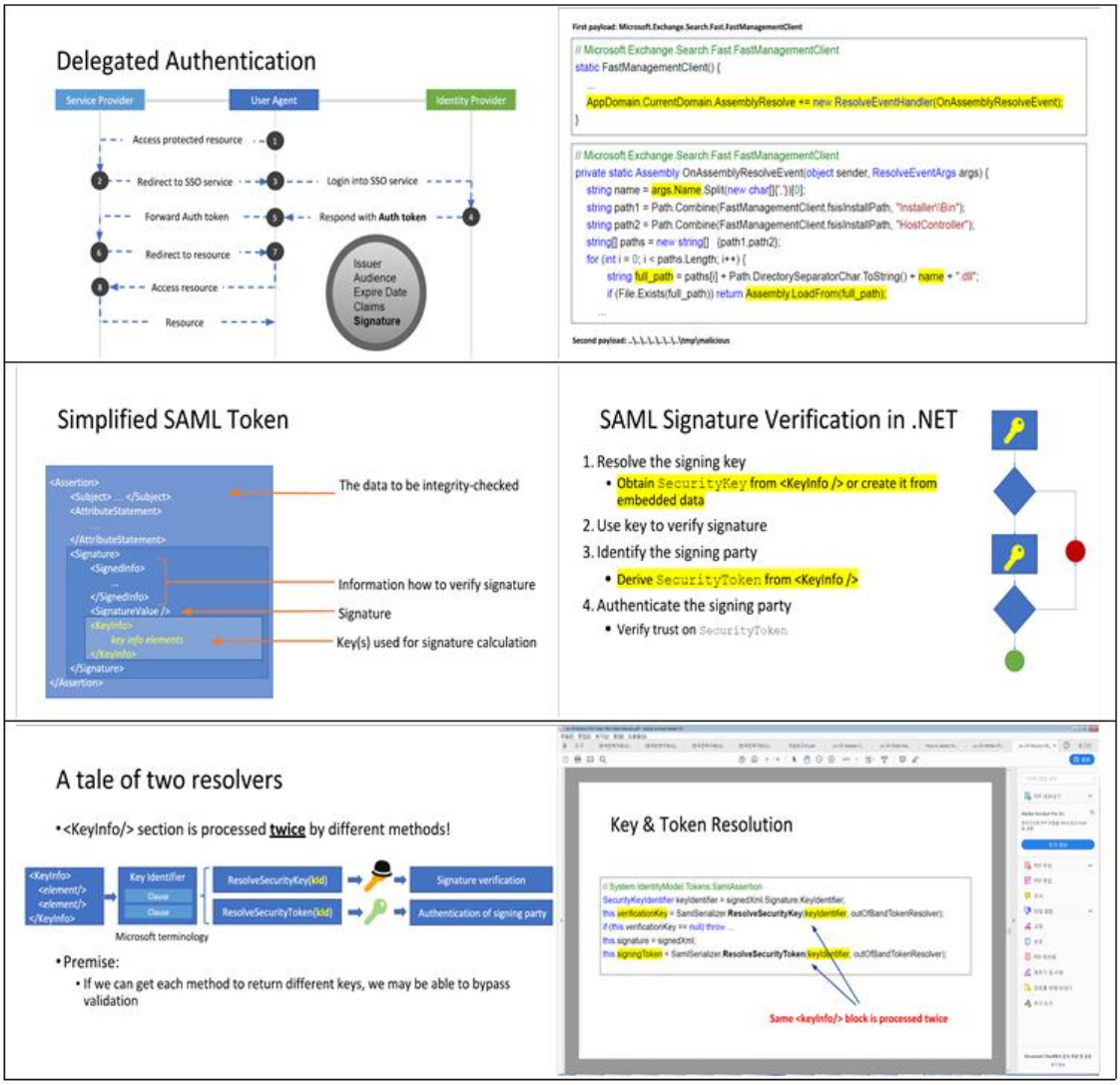
1) 5G 네트워크의 새로운 취약점(New Vulnerabilities in 5G Networks)

- 5G 무선 네트워크의 보안 기능을 분석하고, 운영 인프라와 최종 장치(모바일, BN-IoT, 랩탑 등)에 영향을 미치는 새로운 취약점 발견에 관한 사항
- 저비용 하드웨어 및 소프트웨어 플랫폼을 사용하여 5G /4G 보안 표준의 새로운 취약점을 어떻게 악용할 수 있는지를 설명하고, 실제 평가를 수행하여 보안연구 커뮤니티와 공유할 수 있는 새로운 자동화 도구를 소개
- 전 세계 수 백개의 4G 기지국과 시중에서 판매되는 BN-IoT 프로토콜에서 배터리소모, 하이재킹 등 사용할 수 있는 보안 문제 발표



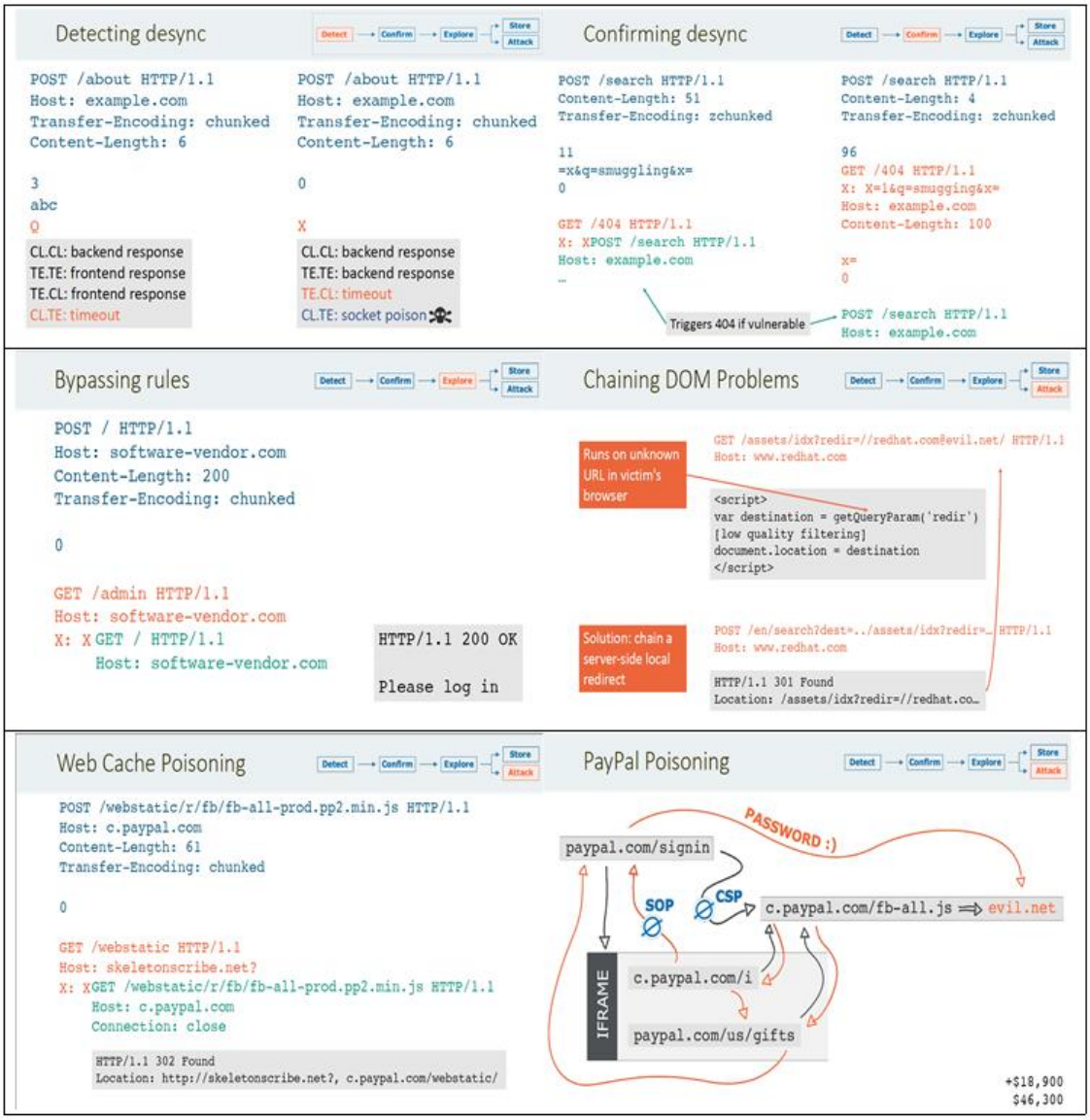
2) SSO 전쟁 : 토큰 위협 (SSO Wars : The Token Menace)

- SSO(Single Sign On)의 안정화 시점에서 새로운 버그가 다양하게 발견되는 현황
- 최근 밝혀진 새로운 두 가지 기술에 대한 소개
  - · XML 서명 유효성 검사를 위반하고 새로운 유형의 SAML 구현 결함으로 공격자가 임의 사용자로 인증하거나, 임의의 권한을 부여 하는 방법
  - · .NET 암호화 라이브러리의 버그로, 공격자가 대상 서버의 가용성(RCE. Remote Code Execution, DoS. Denial of Service)을 제한하는 방법



3) HTTP 비동기 공격 : 다음 셀로 스매싱
(HTTP Desync Attacks : Smashing Into The Cell Next Door)

- 인증되지 않은 원격 공격자가 격리를 통해 스매싱 하고 다른
- 수많은 상업 및 군사 시스템의 웹 인프라, 방문자에 대한 악용이 일어날 수 있음을 설명
- 자신의 요청에 내부 API에 대한 최고 권한을 얻고 웹 캐시를 무력화 하여 가장 신뢰 할 수 있는 로그인 페이지를 탈취하는 방법 설명



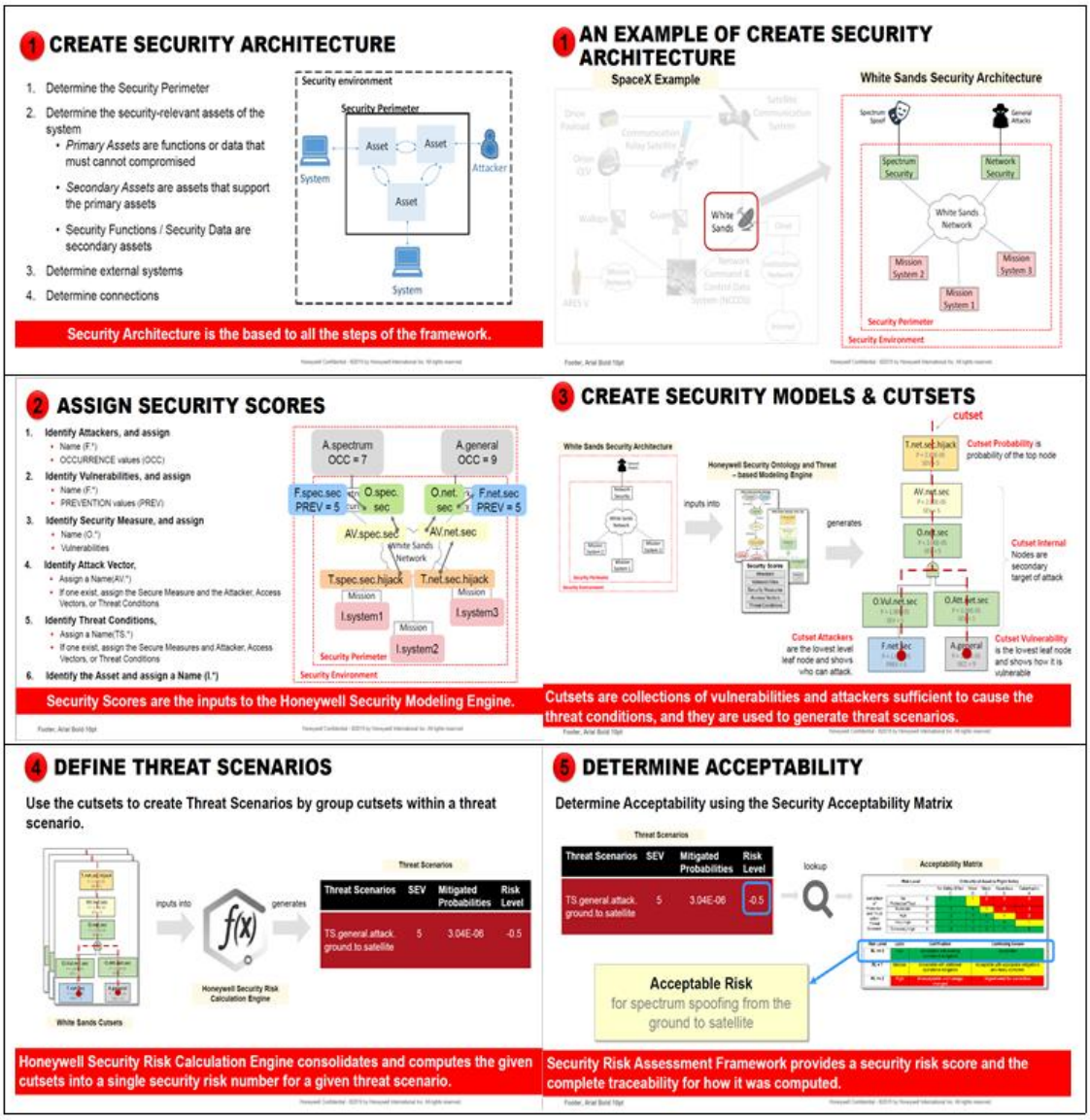
4) DNS를 사용한 도메인 피싱 공격 탐지 기술

(How to Detect that Your Domains are Being Abused for Phishing by using DNS)

- 이메일에서 도메인 사용 권한 부여를 위해 RFC(Request for Comments)를 사용한 피싱 공격 식별 기술 개발
- 이메일의 보안 강화를 위한 고급 옵션(STARTTLS, SPF, DKIM, DMARC, DANE, MTA-STS) 설정 설명
- DNS 로깅에 대한 접근을 전제조건으로 위장한 피싱 공격 탐지를 통해 이메일 피싱 공격 감소 현황 설명

5) 안전이 중요한 시스템에 대한 사이버 보안 위협 평가 (Cyber security Risk Assessment for Safety-Critical System)

- 날씨와 기후 위성에 대한 비즈니스, 정보 위성에 대한 미군의 의존, GPS 위성에 대한 다양한 운송 산업 등 세계 주요 인프라의 대부분은 우주 시스템에 의존
- 우주시스템 보안을 통제하는 표준 형태 및 궁극적으로 이러한 표준이 시행하는 정책 또는 지침이 부재
- 우주시스템에 대한 최근의 주요 사이버 보안 위협에 대한 논의 안전에 중요한 시스템의 보안 위험을 평가

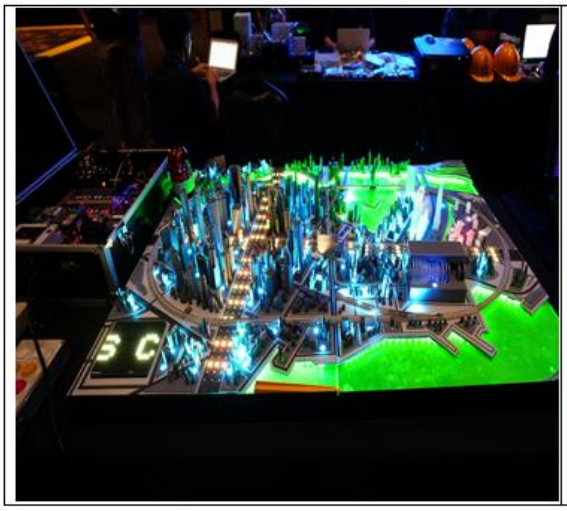


6) BlackHat 2019 주요 활동 사진

나. DEFCON 27 참석

1) 제어시스템 사이버보안 경진대회 특징

- 산업 현장에서 운영중인 장비를 시뮬레이션 모형으로 제작하여 실제 운영 환경을 표현하는 등 현실적으로 발생 가능한 사이버 공격 시나리오 기반으로 대회가 진행
- 문제출제는 산업 시설에 물리적으로 접근하는 단계부터 내부 침입과 네트워크 접근, 망분리 우회, 내부 시스템 공격까지 단계별로 구현
- 산업용 장비의 실존하는 취약점을 이용한 챌린지를 만들어 발전소 가동정지, 기차 탈선, 타워크레인 임의 조작과 같은 문제를 시뮬레이션 모형으로 구현



2) 제어시스템 시뮬레이션을 활용한 경진대회 운영 중점요소

- 경진대회 참가자들이 대회 문제 난이도에 따라 다양하게 도전할 수 있도록 문제를 문제 배분
- 실제 공격 시나리오를 기반으로 제어시스템 시뮬레이션을 구성하여 참가자들이 공격과 방어를 모두 경험할 수 있도록 구성
- 안정적인 대회 운영하기 위해 외부의 어떠한 사이버공격에도 시뮬레이션이나 대회 서버가 오작동 없이 동작할 수 있도록 보안 강화에 중점

3) 제어시스템 시뮬레이션 대회의 효과 분석

- 산업용 제어장비들이 생각보다 보안에 취약하며, 망 분리 환경에서도 우회 요소들이 존재한다는 것을 가시적으로 확인 할 수 있는 장점이 있음
- 시뮬레이션 모형의 피해상황, 복구상황 등을 시각적으로 확인이 가능하여 참가자들의 관심과 동기 부여에 상당한 효과가 있음

4) 경진대회 참여자들의 관심과 호응도 향상방안

- 단순 문제풀이 해킹 대회에서 벗어나 대회를 재미있게 즐길 수 있는 요소(락피킹 등)를 배치하며, 제어설비 침투와 관련된 요소들도 반영하여 호응도를 향상시킬 수 있음

5) DEFCON 27 참석 주요 활동 사진

다. 블룸에너지社 연료전지 엔지니어 실무 회의

1) SOFC type 연료전지의 특징 파악

- SOFC 연료전지는 효율성이 매우 뛰어나며, 상호간 Swap이 가능하고 이중화된 설계로 가동률이 높음
- 최대 가동시간을 제공하기 위해 모듈화 및 결함을 최소화하는 방식으로 설계하여 기업건물 및 주택가에도 설치가 용이
- 연소방식이 아닌 전기화학 반응에 의한 발전으로 자연 친화적

2) 마이크로그리드 시스템의 운영 안정성

- Energy Server는 여러 독립형 전원 모듈로 구성되며, 장애발생시 복구대책을 다양하게 마련
- 마이크로그리드 시스템은 지하 천연가스로 구동되므로 지상의 극한 기후 현상에 대해 취약점이 없이 신뢰성 있는 연료공급 가능

3) 사이버위협 대응활동 및 신재생 보안 가이드라인 적합 여부 검토

- 민간기관의 정보보안 활동 관련 사항으로 기술하지 않음

4) 연료전지 엔지니어 실무회의 사진

4. 출장소감 및 향후 계획

□ Black Hat 2019 기술 전시회 및 컨퍼런스

○ 세계 최대 규모의 글로벌 보안 세미나로 알려져 규모가 상당히 클 것으로 예상은 하였으나, 생각했던 것 이상으로 큰 규모였으며 참가자 또한 상당히 많았음. ISEC, PIS Fair 등 국내의 정보보안 세미나 보다 수 배 이상의 규모임.

○ 수집한 정보보안 최신 기술 및 글로벌 사이버 위협 대응 기술 분석을 통해 보안관제 및 정보보안 업무에 활용 가능함.

구 분	수집 내용
· 모바일 망 연계	New Vulnerabilities in 5G Networks
· 시스템의 SSO 운영	SSO Wars : The Token Menace
· 대국민 서비스 운영	HTTP Desync Attacks : Smashing Into The Cell Next Door
· 피싱 및 스팸 메일 탐지	How to Detect that Your Domains are Being Abused for Phishing by using DNS
· 기반시설 운영	Cyber security Risk Assessment for Safety-Critical System

□ DEFCON 27

○ 제어시스템 사이버 경진대회를 참여자 입장보다 주최자 시각에서 문제 출제 의도 및 방향을 파악 할 수 있었으며, 향후 정부의 제어시스템 및 사이버 경진대회 참여 시 출제자 의도를 파악하여 문제를 풀이 하는데 도움이 될 것임.

○ 폐쇄망 환경에서도 다양한 취약점이 발견 될 수 있으며 사안별 신속한 조치가 가장 중요함을 인지함.

○ 사이버보안 경진대회의 특징을 파악하고 모의해킹 노하우 및 대응기법 습득으로 침해대응 역량을 강화 할 수 있을 것으로 판단됨.

□ 블룸에너지社 연료전지 엔지니어 실무 회의

○ 벤치마킹을 통해 수집한 해외 연료전지 전문기업(블룸에너지社)의 정보보안 환경 및 관제현황을 신재생 에너지 보안에 참고 가능

□ 정보보안 컨퍼런스, 해킹 대회, 블룸에너지 벤치마킹으로 최신트렌드 변화 및 신기술에 대한 정보를 얻을 수 있었고, 향후 제어시스템 보안관리 및 정보보안 현안 업무를 해결하는데 많은 도움이 될 것으로 기대됨.

□ 사이버위협 기술은 지속적으로 변화하며 다양화 되고 있으므로, 최신 기술에 대한 세심한 동향 분석을 통해 사이버 보안 역량 강화 필요.

붙 임. 주요 접촉 인물 현황

이 름	직 위	소 속	이 메 일	비고
Louis Hur	Representative	NSHC	louis@nshc.net	
Park Jeong Woo	Senior Engineer	NSHC	jw.park@nshc.net	
장일수	CEO	SPARROW	ischang @sparrowfasoo.com	
AJ Anderson	Security executive	Dark Trace		
Fred Mitlitsky	Senior Director	Bloom Energy	fred.mitlitsky @bloomenergy.com	
Edward Kim	Director	Bloom Energy	edward.kim @bloomenergy.com	
Van Ryder	Sales Director	Protectwise	sam.vanryder @protectwise.com	
Kristina Zukose	PA Manager	Inductive	kzukose@inductive.com	
Michael Edwards	Director	Venafi	michael.edwards @venafi.com	
kristina cornes	Security Manager	Thycotic	kristina.cornes @p.thycotic.com	
Arturo Gutierrez	Director	bugcrowd	arturo.gutierrez @bugcrowd.com	