‘24년 해외 정보보안 컨퍼런스 출장결과 보고서

‘24. 8

ICT총무처
정보보안부

1. 출장개요

출장목적	2024 해외 정보보안 컨퍼런스 및 해킹대회 참관				
출 장 자	소 속	직급	성 명	당해출장 담당업무	출장경비 부담기관
	ICT총무처 정보보안부	3급	방흥택	최신 보안동향 및 기술 조사	산업통상자원사이버안전센터 지원

2. 출장일정

월일시 (요일)	출발지	도착지	방문기관	담당업무	접촉인물 (직책포함)
08.05 21:00 (월)	인천	-	-	이동(KE0005)	
08.05 16:40 (월)	-	라스베가스	-		
08.06 09:00 ~ 18:00 (화)	라스베가스	라스베가스	전력 에너지시설 Hoover Dam	○ 전력에너지시설 운영 현장 견학 ■ 후버댐 역사 및 건설 과정 관람 ■ 취수 타워, 터널, 수압관, 터빈 시설	
08.07 09:00 ~ 18:00 (수)	라스베가스	라스베가스	Black Hat 컨퍼런스 (Mandalay Bay Hotel)	○ 기조 연설 청강 ■ 민주주의의 가장 큰 해 / 전세계의 안전한 선거를 위한 투쟁 ○ 글로벌 보안 기업 전시 부스 관람 ■ CrowdStrike, Armis, Splunk 등 ■ Darktrace, Palo Alto, Tenable 등 ○ AI 기술을 활용한 사이버 보안 기술 청강 ■ MS, DARKTRACE社 발표	■ 국보연 실장 ■ Sara Metts (Sales Enginneer) ■ Yvonne Le (Marketing Manager) ■ Richard Ybarra (Security Engineer) ■ Brandon Carden (Sales Engineer)

08.08 09:00 ~ 18:00 (목)	라스베가스	라스베가스	Black Hat 컨퍼런스 (Mandalay Bay Hotel)	○ 기조 연설 청강 ■ Fireside Chat with Moxie Marlinspike ○ 글로벌 보안 기업 전시 부스 관람 ■ NOZOMI(OT&IoT), CrowdStrike, Splunk 등 ○ 블랙햇 아스널(ARSENAL) 실습 세션 참여 ■ Metasploit Framework ■ Cloud Offensive Breach and Risk Assessment ■ Hunt for Threats Across Security Data Lakes	■ Andre Heller (Sales Engineering) ■ Tom McKenna (Manager) ■ Norman Laurent (Marketing Manager) ■ Dasha Zenkovich (Marketing Manager) ■ Shail Talati (Senior Director) ■ Simon Ahmet (Sevurity Engineer)
08.09 09:00 ~ 08.11 14:00 (금~일)	라스베가스	라스베가스	DEFCON 32 (LasVegas Convention Center)	○ 다양한 주제/테마별 빌리지 참관 ■ AI, 우주, ICS, IoT, 자동차, 임베디드 시스템, 클라우드, 데이터 복제, 암호화 키, 패킷해킹, RF해킹, H/W 해킹 ○ 기업 홍보 부스 관람	
				○ 다양한 주제/테마별 빌리지 참관 ■ AI, 우주, ICS, IoT, 자동차, 임베디드 시스템, 클라우드, 데이터 복제, 암호화 키, 패킷해킹, RF해킹, H/W 해킹 ○ 해킹 도구, 해킹 시연 Demo Labs 청강 ○ 기업 홍보 부스 관람	
				○ 다양한 CTF 콘테스트 참관 ■ RED ALERT ICS CTF ■ AI, 가상현실 해킹 ■ IoT, 임베디드 Village 등 ○ 해킹 도구 및 시뮬레이터 체험 ○ 기업 홍보 부스 관람	
08.11 23:50 (일)	라스베가스	-	-	이동(KE0006)	
08.13 04:50 (화)	-	인천	-		

3. 업무수행 내용

Ⅰ BlackHat 2024 참관 주요내용

가. 기조연설(Keynote)

- ㅇ 주제 : 민주주의의 가장 큰 해 / 전 세계의 안전한 선거를 위한 투쟁
- ㅇ 연설자 : (미) CISA Director, Jen Easterly
  (EU) ENISA COO, Hans de Vries
  (영) NCSC, Felicity Oswald OBE
- ㅇ 2024년 전세계적으로 많은 대통령 선거가 이뤄지는 세계 민주주의의 해로써 20억명의 유권자가 국가와 세계의 미래를 위해 투표할 것이며 이에 따른 선거 보안은 굉장히 중요한 과제
- ㅇ 4명의 저명인사가 참여한 가운데 민주주의 과정을 방해하려는 시도가 증가하고 있는 상황에서 선거 인프라를 사이버위협으로부터 보호하기 위한 조치에 대해 토론함.
- ㅇ 그 결과 사이버 공격을 통해 선거 결과를 직접 조작할 가능성은 낮지만 실제 위협은 선거 과정에 대한 대중의 신뢰를 훼손하도록 고안된 잘못된 정보의 확산, 즉 가짜 뉴스에 위험이 있으며 이들의 목적은 직접적인 피해보다 혼란과 의심을 조성하기 위함.

나. 비즈니스홀

- ㅇ 올해 행사에서는 아이덴티티 및 접근관리(IAM)의 중요성이 부각되고 인공지능(AI)과 클라우드 보안의 진화에 이르기까지 여러 주제가 전시
- ㅇ 아이덴티티 및 접근 관리(IAM)의 중요성
  - 자격 증명의 유출과 아디덴티티 기반 공격이 증가함에 따라 접근관리는 이제 최우선 과제로 자리 잡았음.
  - 이번 행사에서는 강력한 접근관리의 실천이 민감한 데이터를 보호하고, 오직 권한이 부여된 사용자만이 중요한 시스템에 접근할 수 있도록 보장하는데 필수적이라는 점이 강조됨

- 클라우드 시대의 요구에 맞춰 접근관리 기술에 대한 대규모 투자가 계획되는 전환점을 의미함.

ㅇ 보안 운영에서의 인공지능(AI) 도입

- 인공지능(AI)은 수년간 Black Hat에서 화제가 되어 왔지만 올해 행사에서는 이론적인 논의에서 벗어나 실용적인 전환을 반영하였음.
- 이제 AI는 단순한 이론이 아닌 위협 탐지와 대응 자동화, 전반적인 보안 태세 개선 등 기존 보안 프레임워크에 통합될 수 있는 도구로 자리 잡았음.
- 특히, 사이버안전센터에서 사용하고 있는 Splunk 제품과 관련하여 AI기술로 질문에 대한 답변을 주는 것을 확인하였음.
- 이는 생성형 AI기술과 대규모 언어모델(LLM)을 이용하는 것으로 데이터의 확보, 지속적인 신규 위협에 대한 학습 등이 주요한 숙제인 것으로 보이나 10월경 출시되는 제품에 대해 관심있게 볼 필요가 있음.

ㅇ 지속되는 클라우드 보안의 과제

- 코로나19 이후 클라우드 전환이 가속화 됨에 따라 클라우드 환경의 보안은 여전히 중요한 과제임.
- 행사장에서는 클라우드 환경을 보호하기 위한 새로운 도구와 모범 사례들이 소개되었으며, 특히, 제로트러스트 아키텍처(ZTA)와 최소 권한 액세스 모델이 강조 되었음.
- 예전엔 클라우드가 고급 기술이었으나 최근에는 클라우드 공격도 보편적인 기술이 되었으며 점점 더 클라우드 공격이 늘어나는 추세
- 클라우드 인프라가 더욱 복잡해지고 비즈니스 운영의 중심이 됨에 따라 이를 완전히 보호하기 위해서는 많은 과제가 남아 있음

ㅇ 조직 회복력 및 데이터 보안의 중요성

- 최근 크라우드스트라이크 IT 장애와 같은 심각한 사고로 조직의 회복력은 이제 많은 기업의 주요 관심사
- 많은 기관들은 미래의 위협에 대응할 수 있는지 확인하기 위해 기존 플랫폼을 면밀히 검토하고 있으며, 적응력과 회복력이 있는 보안조치가 필요하다고 강조

다. 참관사진

<컨퍼런스 및 해킹대회 참관 단체사진>

<BlackHat 컨퍼런스장 단체사진>

<BlackHat 주요 행사>

<BlackHat 출입증>

<Spear-phishing 예제>

<AI 보안 관련 청강>

<솔루션 데모 확인>

<보안솔루션 청강>

<클라우드 보안 솔루션 청강>

<AI 보안 관련 보안취약점 청강>

<부스 방문>

<부스 체험>

Ⅱ DEFCON 32 참관 주요내용

가. DEFCON 32 특징

○ ‘93년 유명 해커인 제프모스(Jeff Moss)에 의해 설립된 세계에서 가장 큰 해커들의 축제로, 보안 컨퍼런스 및 해킹대회 등으로 구성

○ 주어진 문제를 풀어서 점수를 획득하는 방식의 CTF콘테스트 외 다양한 주제 발표, 여러 분야별* 체험관, 해킹시연, 마켓 오픈 등

* AI, 우주, ICS, IoT, 자동차, 임베디드 시스템, 클라우드, 데이터 복제, 암호화 키, 패스워드크랙, HAM 라디오, H/W 해킹

나. DEFCON 국제해킹대회

○ 미국 사이버보안 학술회의인 DEFCON 행사 기간에 열리는 세계 최고의 해킹대회로 8월8일~11일 미국 라스베가스에서 본선대회 개최

○ 5월 총 263개 팀이 참여하여 12팀이 본선에 진출하였으며, 이중 5개 팀*은 모두 국내 최고 화이트해커 양성 프로그램인 차세대 보안지도자 양성프로그램(BoB)** 수료생 및 담당 지도자들로 구성

* Maple Mallard Magistrates(MMM), SuperDiceCode, HypeBoy, Cold Fusion, Friendly Maltese Citizens

** 정보보호 최고 전문가로 구성된 멘토들의 맞춤형 교육과 팀 프로젝트 등으로 구성된 약 9개월간의 교육을 진행하고 있으며 美데프콘 5회('15, ‘18, ’22, ‘23, ’24) 우승 등 우수한 성과 달성

○ 이번 대회에서 MMM팀이 우승하였으며 지난 ‘22년부터 3년 연속 1위를 차지하며 그 실력을 전 세계에 입증하였음.

< MMM팀 개요 >

▸ 차세대 보안지도자 양성 프로그램(BoB) 책임 담당 지도자인 박세준 대표와 수료생으로 이루어진 국내팀(The Duck, 29명)과 미국(PPP), 캐나다(Maple Bacon)팀이 연합하여 구성(총 50명)
▸ ’22, ’23, ’24년도 DEFCON CTF 연속 1위

다. 주요 체험관(Villages)

○ 물리보안 체험관에서는 쇠붙이를 이용해 잠겨진 문을 여는 것을 체험

- ICS 체험관에서는 물펌프 제어, 전력망 제어, 풍력 발전기 제어 등의 시뮬레이션들이 전시되어 있으며 다수의 참가자들이 이에 대한 CTF 취득을 위한 해킹 시도가 이루어 짐
- 항공 빌리지에서는 비행기, 우주선 등을 탈취하는 해킹 시연이 있음.
- AI 체험관에서는 송출 화면에 위조하여 가상의 인물을 만들어 내는 시연이 있음.
- 패킷 해킹 빌리지에서는 해킹에 필요한 기본적인 정보를 제공한 후 패킷을 해킹하는 시연이 이루어지고 있음.
- 자동차 해킹 빌리지에는 2대의 자동차가 전시되어 있으며 이에 대한 CTF를 획득하기 위해 해커들의 시도가 있음.
- 레트로 빌리지에는 구형 PC들이 전시되어 있으며 이를 개선하여 최근 3D 게임을 플레이하는 시연을 보여줌. 오래된 PC라도 해킹이 가능함을 보여주는 사례
- 슈퍼 선거의 해답게 투표 관련 개표기에 대한 해킹시연도 전시되었음. 실제 개표기가 전시되어 있고 이에 대한 해킹 시연이 있음.
- 이외데오 클라우드, IoT, 패스워크, RF(무선) 해킹 등 다양한 빌리지를 방문하여 체험해 볼 수 있는 기회가 제공됨.

라. 참관사진

<DEFCON32 참관 단체사진>

<DEFCON 행사장>

<패킷 해킹 빌리지>

<패킷 해킹 빌리지>

<물리적 해킹 빌리지>

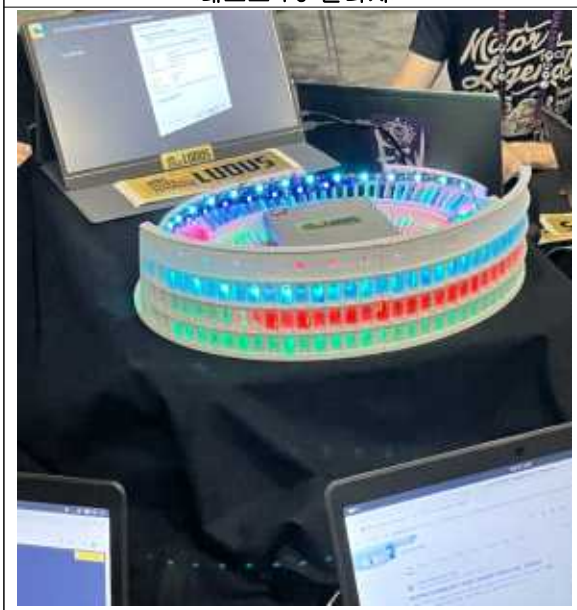
<AI 빌리지>

<클라우드 보안 솔루션 청강>

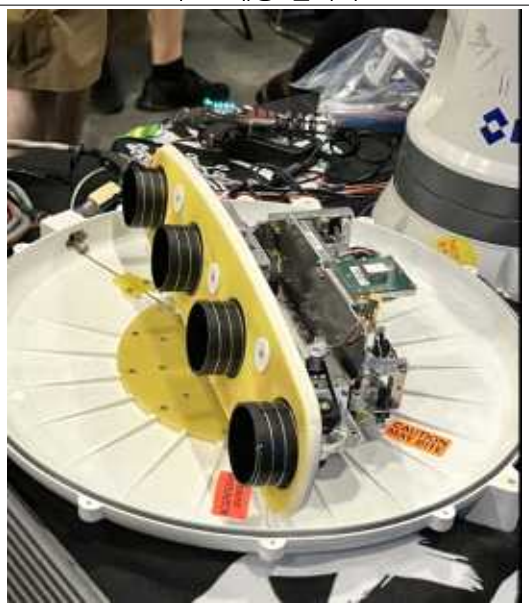
<자동차 해킹 빌리지>

<레트로 PC 빌리지>

<투표 해킹 빌리지>



<임베디드 빌리지>



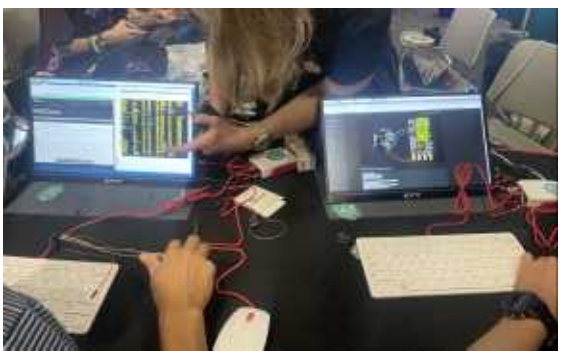
<항공 빌리지>

<ICS 빌리지 - 물펌프 모형>

<ICS 빌리지>

<ICS 빌리지 - 풍력발전기 모형>

<ICS 빌리지>



<실제 해커들 시연>

<투표 해킹 빌리지>

Ⅲ 후버댐(HooverDam) 전력에너지 시설 견학

가. 후버댐 역사와 기능

ㅇ 미국은 1929년 이후 발생한 대공황 극복 위해 후버댐 건설(1931년~1935년)

ㅇ 안정적인 수자원(콜로라도강 홍수 조절, 갈수기 물 확보) 관리

ㅇ 총 2,080MW의 발전 용량으로 캘리포니아, 네바다, 애리조나 전력 공급

나. 전력 생산 시설

ㅇ 4개의 취수 타워에서 끌어올린 물의 운동 에너지를 높이기 위해 긴 수압관을 통과한 후 얻은 수압을 이용하여 수직 터빈을 가동

ㅇ 발전용 터빈은 총 17개이며, 양쪽으로 분리(8개, 9개)되어 운영

다. 사이버위협 대응방안

ㅇ 제어 시스템은 다른 일반 IT 지원 시스템 및 인터넷과 격리되어 있음

ㅇ 외부 장치를 통한 악성코드 감염을 방지 및 보호하기 위한 제어 구현

ㅇ 내부자 해킹 위협을 대비하여 시스템 권한이 있는 개인에 대한 엄격한 조사와 제어 시스템에 대한 관리자 권한 접근을 철저히 통제하고 있음

<후버댐 발전 시설 모형>

<후버댐 터빈 모형>

4. 출장성과 · 시사점 및 향후 업무 활용 계획

- ㅇ 이번 출장을 통해 최신 보안 위협 동향 및 공격 기법에 대해 심도 있게 이해할 수 있었음.

  특히, 최근 부각되고 있는 AI, 클라우드, 복원력에 대한 정보를 얻었으며, 이는 향후 보안 전략에 중요한 참고자료가 될 것.
- ㅇ 몇 년간 심도있게 논의 된 ‘AI’, ‘클라우드’, ‘복원력’ 에 대한 보안에 대한 내용이 최근 구체화 되고 전반적인 개선을 위해 기존 보안 프레임워크에 통합할 수 있는 방안이 고민되고 있음.
- ㅇ 최근 ‘크라우드스트라이크社’의 보안사고에서 볼 수 있듯이 현실에서 사고로 이루어지는 만큼 이에 대한 적응력과 복원력 향상을 위한 방안이 지속적으로 개선되어야 함.
- ㅇ 컨퍼런스 데모를 통해 AI와 클라우드 보안 관련 제품 출시가 예고된 만큼 관련 보안 제품에 대한 동향과 성능을 관심있게 살펴보아야 하며 필요시 해당 시스템 도입을 검토 및 제안을 추진
- ㅇ 해킹대회 참관을 통해 일상생활 전반에 걸친 모든 분야에 해킹이 일어날 수 있다는 것을 인지 하였고, 기본적인 사항부터 세부적인 내용까지 보안성 강화를 추진해야겠음.
- ㅇ 향후 AI 보안관제 및 해킹방어 대회 등 업무 개선 활동에 적극 반영 예정
- ㅇ 미국의 보안 정책 변화(보안투자 인센티브 등)에 따라 정부의 정보보안정책 변경사항을 반영하여 우리공사 정보보안 정책에 반영할 필요가 있음.

5. 출장경비

- ㅇ 국외경비 : 산업통상자원사이버안전센터 비용 지원. 끝.