

산업부 주관 정보보안 컨퍼런스 참여 공무 국외출장 결과보고서

- '25.08.29. 정보보안실 -

1. 출장 개요

□ 출장기간 : 2025.8.5.(화) ~ 8.13.(수) [6박 9일]

□ 출 장 지 : 미국(라스베가스)

□ 출 장 자 : 정보보안실

□ 출장 목적

- 1) 신규 해킹 기법 · 분석방안 등 최신 정보보안 기술 및 동향 파악
- 2) 해외 기반시설 견학을 통한 해외 제어시스템 보안 업무 파악

□ 주요일정

| 일 자 | 주요 일정 | 비고 |
|----------------------|--|----------------|
| 8.5(화) | ◦ 집결: 인원파악 및 공지사항 (인천공항 18:00) ◦ 이동: 인천(ICN, 21:00) → 라스베이거스(LAS, 16:40) - 약 11시간 40분 소요 | 공항 → 숙소 |
| 8.6(수) ~ 8.7(목) | ◦ Black Hat USA 2025(8.2~8.7) 등록 및 참관 - 보안제품 및 솔루션 전시회와 컨퍼런스 - 약 2만여명 IT 및 보안전문가 참석하여 보안관련 정보 공유 | 숙소↔컨퍼런스 |
| 8.8(금) ~ 8.10(일) | ◦ DEFCON 33(8.7~8.10) 등록 및 참관 - 세계최대 해킹대회 (보안 컨퍼런스 및 해킹대회 등으로 구성) - CTF콘테스트(주어진 문제를 풀어서 점수를 획득하는 방식) - AI, IOT, ICS, Cloud, Encryption 등 분야별 체험관, 해킹 시연, 해킹도구 마켓 운영 등 | 숙소↔컨퍼런스 |
| 8.11(월) ~ 8.13(수) | ◦ Hoover Dam 발전시설 견학 - 취수 타워, 터널, 수압관, 터빈 시설 등 견학 및 사이버위협 대응방안 청취 ◦ 이동: 라스베이거스(LAS, 23:50) → 인천(ICN, +2, 04:40) - 약 12시간 50분 소요 | 숙소→견학장소 →공항 |

2. 출장 수행 내용

□ BlackHat 2025 참관

1) 기조연설(Keynote)

- 주제 : 지난 30년간의 사이버 공격 진화사와 미래 위협 전망
 - 연설자 : WithSecure 최고연구책임자, Mikko Hypponen
 - 사이버 위협의 진화: 1990년대 초반의 스톤드와 같은 초기 바이러스부터 코드레드, 슬래머, 컨피커, 스텍스넷, 워너크라이, 록빗과 같은 현재의 주요 사례에 이르기까지 사이버 공격 사례 분석 및 진화 과정 설명
 - 보안의 중요성: 사이버 보안은 단순히 컴퓨터를 보호하는 것이 아닌 사회를 보호하는 것이며, 사이버 보안이 단순한 기술적 문제를 넘어 사회적, 경제적 문제로 확산되고 있음을 강조
 - 미래 예측: AI와 자동화 기술의 발전이 사이버 공격에 미치는 영향을 예측하고, 이에 대한 대응 전략 제시
- 주제 : 새로운 최전선-벼랑 끝에 선 사이버
 - 연설자 : Silver Buckshot Ventures의 Founding Partner, Nicole Perlroth
 - 공격표면의 변화: 단순 코드나 인프라 → 사람, 기관 등으로 현재의 사이버 공격 표면 변화 설명
 - 사이버위협 변화: 전통적인 사이버 공격에서 벗어나, AI 기반의 자동화된 공격으로의 전환을 설명(사이버위협 모듈화, 자율화 언급)
 - AI의 역할: AI가 사이버 공격의 효율성을 높이는 동시에, 방어 측의 대응을 어렵게 만드는 양면성을 지니고 있음을 강조
 - 미래 전망: 사이버 보안의 미래를 예측하며, 기업과 정부의 대응 전략에 대한 통찰을 제공

2) 비즈니스홀

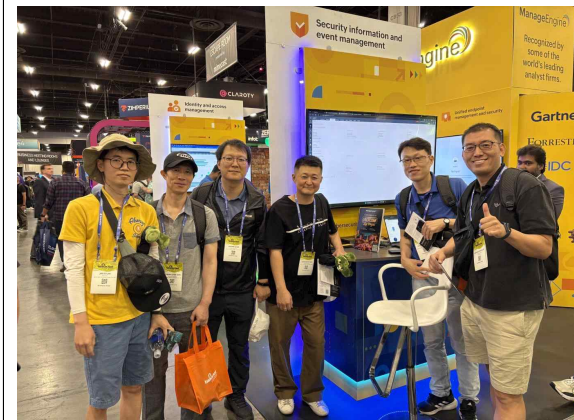
- 올해 행사에서는 인공지능(AI)과 SOC(보안운영센터) 운영, 클라우드 보안의 진화에 이르기까지 여러 주제가 전시
- 2025년 위협 탐지 보고
 - 전자 범죄 및 국가 차원의 공격자들이 사용하는 최첨단 수법 소개

- 해커들의 크로스 도메인 공격 악용 방법 등 실제 침입 사례 소개
- 인공지능(AI) 기반 보안 운영
 - 적대적AI 대응 솔루션: 사이버 범죄를 획기적으로 발전시켜, 숙련도가 낮은 공격자조차 딥페이크를 제작할 수 있게 함에 따라 최신 AI 기반 전술 분석을 통한 선제적 위협 대응이 가능한 솔루션 소개
 - AI 스택 해킹 방지: AI시스템과 대규모 언어 모델(LLM)을 보호하기 위한 보안 접근방법 소개, OWASP LLM TOP10 분석 기반으로 딥페이크와 제로데이 공격으로부터 AI 스택 보호 방법 소개
 - 보안 분야 AI 성숙도 향상: 위협 탐지, 경고 분류, 취약성 관리, 사고 대응 등 핵심 보안 기능 전반에 대한 성숙도 모델 적용 방법 소개, 안정적으로 확장 가능한 AI 시스템 설계 방법 소개
- SOC(보안운영센터)
 - SOC 분석 역량 향상: 전체 보안 스택에서 AI를 활용할 수 있도록 지원할 수 있도록 SOC에 AI 적용 방식 소개
 - SOC 구축 방법: 해커들이 방어 도구를 우회해서 침투하고 있음에 따라, 하이브리드 공격의 구조를 분석하여 기존 도구의 우회 지점을 찾아 해커가 악용하는 탐지 허점을 해소하는 방식으로 SOC 구축 방법 소개
 - SOC의 에이전트 AI: 다중 에이전트 AI프레임워크를 구축하여 분석가의 업무 부담 감소 및 정확도 향상 방안 소개
- 클라우드 보안
 - 클라우드 보안: 데이터 추적, 서비스와 앱의 취약점 악용 등 공격 방식 공유 및 멀티 클라우드 환경 보호를 위한 보안정책·제어 방안 수립 방법 소개
 - SaaS 및 AI 앱 보안: SaaS 앱 공격 방식 설명, 지속적인 SaaS 및 AI 보안 프로그램 구축·운영을 위한 프레임워크 소개
- 데이터 보안
 - 위협 환경에서의 제로 트러스트 및 데이터 복원력: AI 거버넌스, 제로 트러스트 아키텍처, 지속적 제어 모니터링(CCM) 전략 소개
 - 데이터 거버넌스: AI 시스템 구축에 앞서 데이터 거버넌스의 필요성 및 사례 소개, 데이터 거버넌스를 구축하는데 필요한 조직 프레임워크, 정책 및 도구 소개

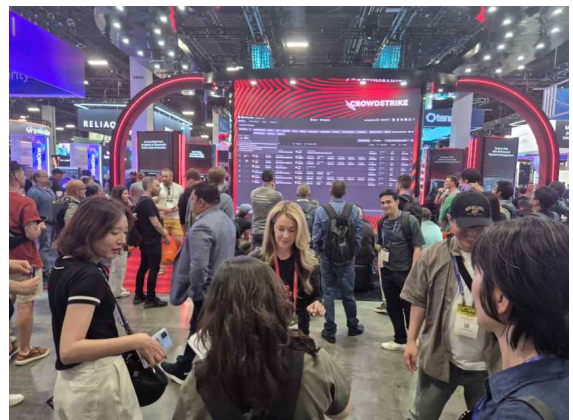
3) 참관사진



<BlackHat 컨퍼런스 참관 단체사진>



<BlackHat 주요 행사 참관>



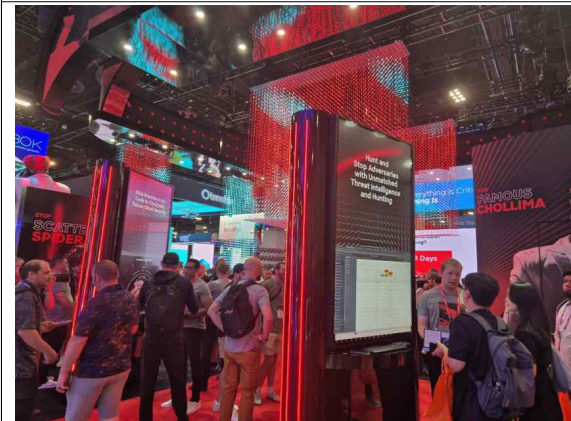
<비즈니스홀 행사장>



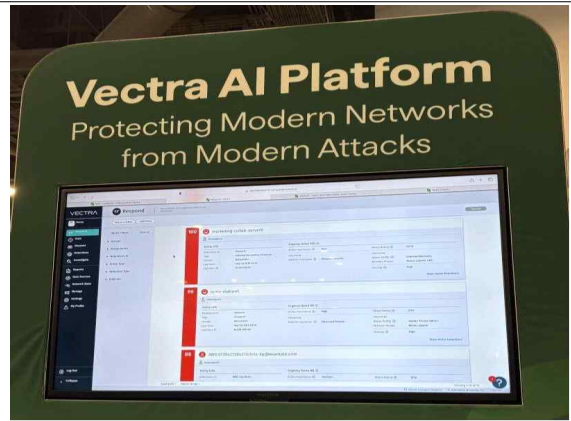
<CROWDSTRIKE社 2025 위협 탐지 보고 청강>



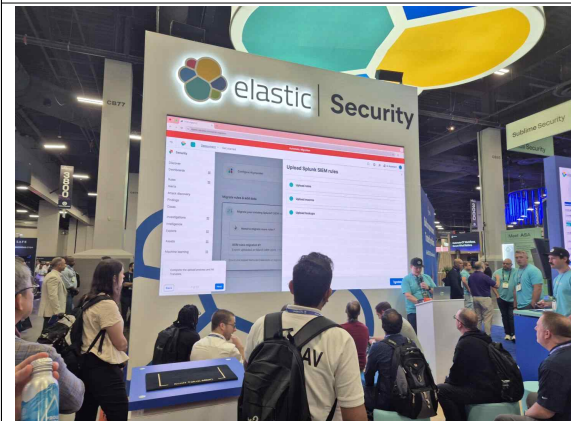
<보안 자동화 · 통합 솔루션 청강>



<클라우드 기반 차세대 엔드포인트 보안 플랫폼 청강>



<AI 기반의 네트워크 방어 중심 NDR 청강>



<클라우드 보안 솔루션 청강>



<소프트웨어 공급망 보안 청강>



<부스 방문>



<부스 체험>

□ DEFCON33 참관

1) DEFCON 33 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

2) DEFCON 국제해킹대회

- 미국 사이버보안 학술회의인 DEFCON 행사 기간에 열리는 세계 최고의 해킹대회로 8월 7일~10일 미국 라스베이거스에서 본선대회 개최
- 4월 총 195개 팀이 참여하여 12팀이 본선에 진출하였으며, 이 중 4개 팀*은 모두 국내 최고 화이트해커 양성 프로그램인 차세대 보안지도자 양성프로그램(BoB)** 수료생 및 담당 지도자들로 구성
 - * Maple Mallard Magistrates(MMM), SuperDiceCode, 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, '25) 우승 등 우수한 성과 달성
- 이번 대회에서 MMM팀이 우승하였으며 지난 '22년부터 4년 연속 1위를 차지하며 그 실력을 전 세계에 입증

< 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, '24, '25년도 DEFCON CTF 연속 1위

3) 주요 체험관(Villages)

- AI 체험관에서는 AI 기술을 활용하여 CTF 문제를 풀 수 있도록 웹 페이지 제공, 딥페이크 시연 및 실시간 데모를 통한 AI 기반 위협 탐지 및 분석 소개
- 물리보안 체험관에서는 쇠붙이를 이용해 잠겨진 문을 여는 것을 체험

- 악성코드 빌리지에서는 의료 데이터 표준(DICOM) 포맷을 악용한 새로운 악성코드 전달 기법을 다루고 있으며, Polyglots 파일 기법을 활용하여 보안 탐지를 우회하는 방법을 시연
- 모바일 해킹 빌리지에서는 Android APK 구조를 분석하고, 덤핑크 또는 조건 기반 로직을 우회하여 플래그 메모리에서 획득하는 리버스엔지니어링 실전 기법 시연
- 하드웨어 해킹 빌리지에는 Hands-on Hacking Challenge 종류의 물리보안과 전자공학 및 논리 퍼즐이 결합된 실습형 해킹 체험이 가능
- ICS 체험관에서는 물펌프 제어, 전력망 제어, 풍력 발전기 제어 등의 시뮬레이션들이 전시되어 있으며 다수의 참가자들이 이에 대한 CTF 취득을 위한 해킹 시도가 이루어 짐
- 버그 바운티 체험관에서는 실제와 유사한 웹앱, API 등을 대상으로 버그를 발견하고 리포트 작성·제출 시, 보고서 품질에 따라 점수 추가 지급받는 방식으로 체험 가능
- 패킷 해킹 체험관에서는 네트워크 패킷을 분석하여 문제를 푸는 체험이 가능하며 네트워크 포렌식 강연 진행
- 피싱 스토리 체험관에서는 소셜 엔지니어링+글쓰기를 결합한 콘테스트로 가상의 기업 리더를 표적으로 삼는 설득력 있으면서 유쾌한 피싱 이메일을 작성하고 리포트를 제공하는 방식으로 체험 가능
- 임베디드 체험관에서는 임베디드 시스템의 펌웨어 또는 하드웨어 취약점을 이용하여 장치에 접근 또는 제어하는 해킹 체험 가능
- 사이버 방어 체험관에서는 제조, 유틸리티, 국방, 금융 등 특정 산업/부문에 초점을 맞춘 시나리오 기반으로 유입되는 공격에 대해, 네트워크에서 발생하는 비정상 이벤트 탐지·대응, 분석, 복구하는 방식으로 내부 네트워크 및 시스템을 방어하는 체험 진행
- 이외에도 항공우주, 자동차, 선박, 클라우드, 패스워드, RF(무선), IoT, 코드 브레이커 등 다양한 분야의 해킹 빌리지를 방문하여 체험해 볼 수 있는 기회가 제공됨

4) 참관사진



<DEFCON33 참관 단체사진>



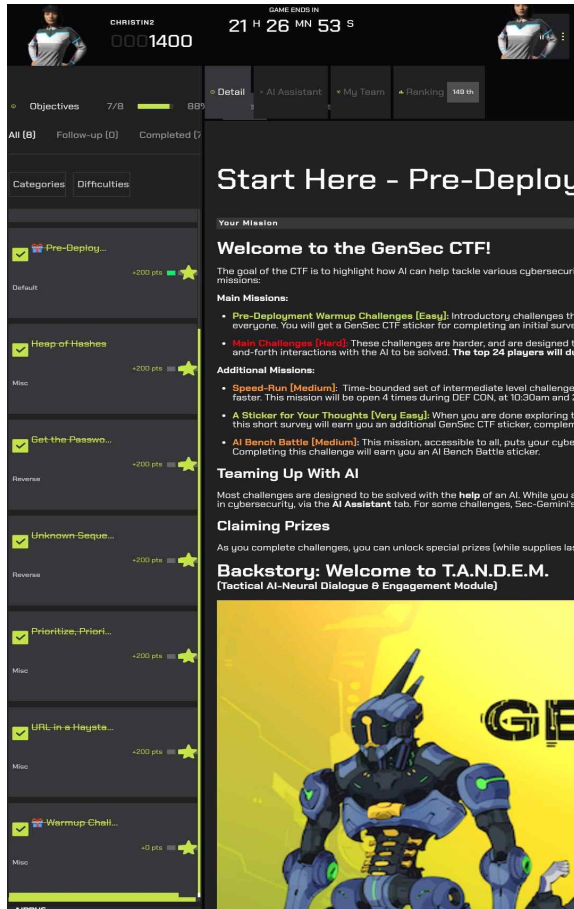
<DEFCON 행사장 안내>



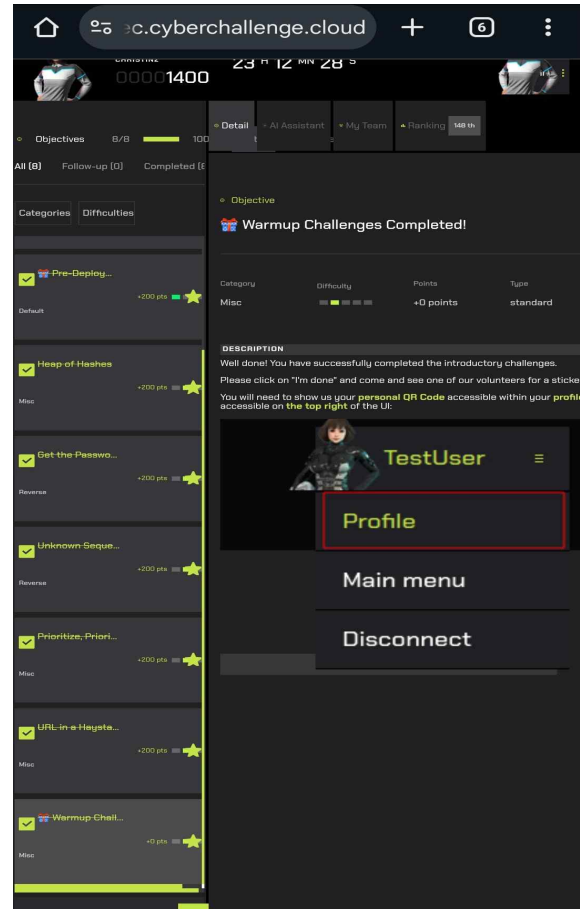
<Hands-on Hacking Challenge>



<Hands-on Hacking Challenge>



<GenSec CTF 참여>



<GenSec CTF 참여>

□ 후버댐(HooverDam) 전력에너지 시설 견학

1) 후버댐 역사와 기능

- 미국은 1929년 이후 발생한 대공황 극복 위해 콜로라도강의 블랙 협곡을 막아 후버댐 건설(1931년~1935년)
- 안정적인 수자원(콜로라도강 홍수 조절, 갈수기 물 확보) 관리
- 총 2,080MW의 발전 용량으로 캘리포니아, 네바다, 애리조나 전력 공급
- 1940년 댐 구조물의 성능 시험과 1983년 홍수 발생 때 2번의 후버댐 방류 시행
- 가뭄으로 인하여 미드 호의 수위가 낮아짐에 따라 발전량도 많이 낮아진 상황이나 2023년부터 수위 회복 중

2) 전력 생산 시설

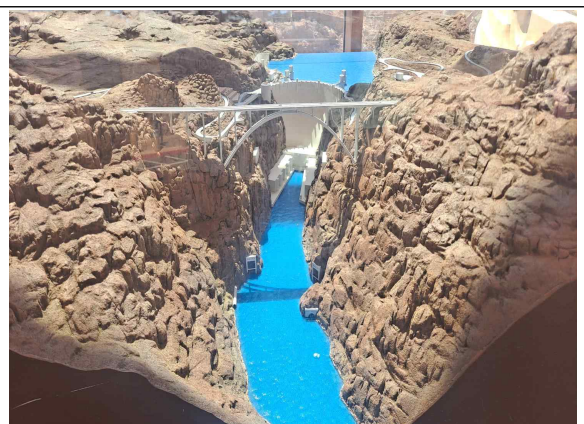
- 4개의 취수 타워에서 끌어올린 물의 운동 에너지를 높이기 위해 긴 수압관을 통과한 후 얻은 수압을 이용하여 수직 터빈을 가동
- 발전용 터빈은 총 17개이며, 양쪽으로 분리(8개, 9개)되어 운영

3) 사이버위협 대응방안

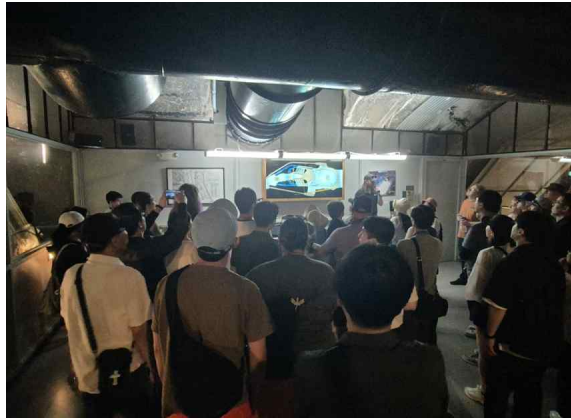
- 제어 시스템은 다른 일반 IT 지원 시스템 및 인터넷과 격리되어 있음
- 외부 장치를 통한 악성코드 감염을 방지 및 보호하기 위한 제어 구현
- 내부자 해킹 위협을 대비하여 시스템 권한이 있는 개인에 대한 엄격한 조사와 제어 시스템에 대한 관리자 권한 접근을 철저히 통제하고 있음



<후버댐 전경>



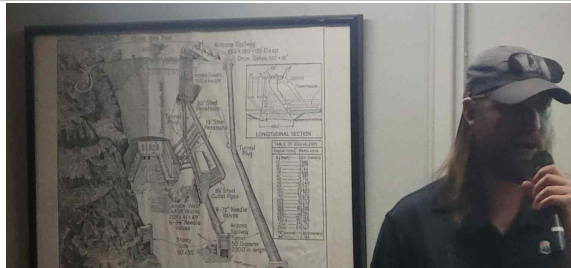
<후버댐 모형>



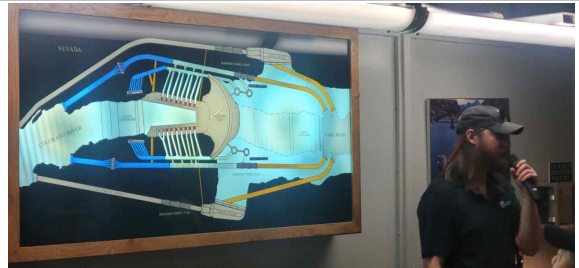
<후버댐 발전 원리 설명>



<후버댐 발전 원리 경청>



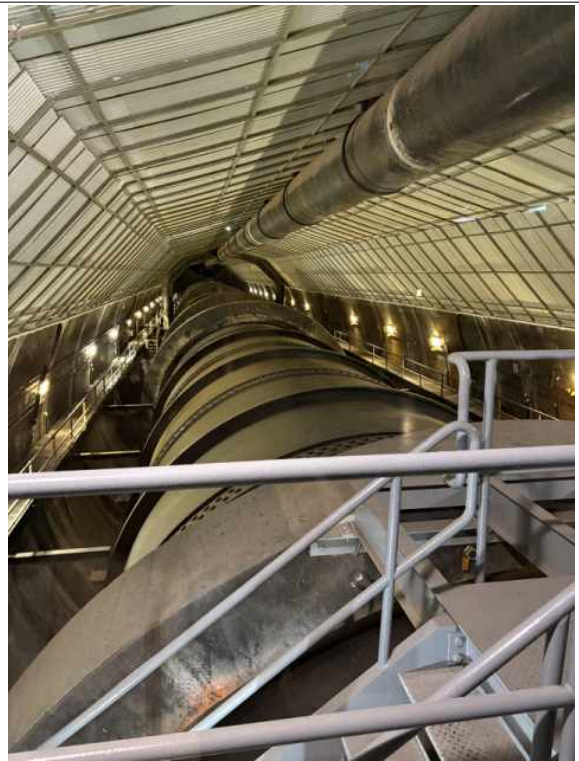
<후버댐 구조와 시공 방법>



<후버댐 발전 원리 설명>



<후버댐 발전기>



<후버댐 펜스톡>

3. 출장소감 및 시사점

□ BlackHat 2025 참관

- 세계 최대 규모의 글로벌 보안 세미나로 알려져 규모가 상당히 클 것으로 예상은 하였으나, 생각했던 것 이상으로 큰 규모였으며 참가자 또한 상당히 많았으며 ISEC, PIS Fair 등 국내 정보보안 세미나 보다 수 배 이상의 규모임
- 최신 보안 위협 동향 및 공격 기법을 파악할 수 있었으며 기관 내 보안 관제 및 정보보안 전략 수립에 활용 예정
 - 다양한 침해사고 사례에서 언급하듯 대응 관점뿐 아니라 복원 관점에서도 접근할 필요성이 있기 때문에 백업·복구 훈련 횟수 증가 등의 방식으로 복원력 강화 필요
 - 보안관제시스템 운영에 AI 시스템을 적용하여 이벤트 분석 업무 감소 및 정확도 향상 필요. 단, 단순 AI 시스템 적용이 아닌 AI 프레임워크 구축 방식으로 접근 필요
 - 데이터 거버넌스에 대한 필요성 인식 및 중장기 정보보안 전략 수립 시 해당 내용 반영 필요
 - 제로 트러스트 방식을 기관에 적용 시 컨퍼런스의 아키텍처 참고 가능
 - 다양한 외산 제품 및 솔루션 소개가 있었으나, 우리기관은 기반시설임에 따라 선별이 필요하며 지속적인 제품 모니터링을 통하여 필요시 시스템 도입 검토 추진

□ DEFCON33 참관

- 다양한 분야에 대한 해킹 체험관이 마련되어 있어 참가자들의 흥미를 일으켰으며, 실제 체험을 통하여 역량 강화에 도움이 되었음
- 사회공학부터 항공우주까지 사회 전반에 걸친 모든 분야에 해킹이 일어날 수 있다는 경각심을 가지게 되었으며, 기관의 보안 프로세스를 재검증하고 프로세스 전반에 걸쳐 강화 및 고도화 추진 필요성을 깨달음
- 특히, ICS 체험관을 통해서 폐쇄망 환경에서도 다양한 취약점이 발견될 수 있으며 사안별 신속한 조치가 가장 중요함을 다시 한 번 인지하는 계기가 됨

- 사이버보안 경진대회의 특징을 파악하고 모의해킹 노하우 및 대응기법 습득으로 침해대응 역량을 강화할 수 있을 것으로 판단됨

□ 후버댐(HooverDam) 전력에너지 시설 견학

- 국가 기반시설의 안정적 운영은 단순 전력 생산이 아닌 사회 전체의 안전과 직결됨을 다시 인지하는 계기가 되었음
- 또한, 실제 현장을 보며 사이버 위협이 단순한 IT 문제로의 접근이 아닌 국가 안보 차원에서 접근해야 함을 체감함
- 후버댐 견학 시, 까다로운 출입통제 절차를 거쳤는데 이를 통해 물리적 보안과 사이버 보안이 동시에 강화되어야만 전체적 리스크를 감소시킬 수 있음을 깨달음
- 미국의 전력망 보안 정책과 같이 우리나라도 발전·송배전 등 기반시설 분야별 특화 사이버보안 규제 및 합동 훈련, 국제 협력 체계 필요성을 체감함

붙임. 주요 접촉 인물 현황

| 순번 | 이름 | 직위 | 소속 |
|----|------------------|--|--------------------------|
| 1 | Mikko Hypponen | Chief Research Officer | WithSecure |
| 2 | Snehal Antani | CEO | Horizon3.ai |
| 3 | Nicole Perloth | Founding Partner | Silver Buckshot Ventures |
| 4 | Aarti Borkar | Corporate Vice President | Microsoft |
| 5 | Peter Prizio | Head of Threat Detection Technology Engineering | Splunk |
| 6 | Michael Sikorski | CTO | PaloAlto Networks |
| 7 | Lucie Cardiet | Cyberthreat Research Manager | Vectra AI |
| 8 | John Peterson | Chief Development Officer | Sophos |
| 9 | Tony De Bos | Vice President | Kyndryl |
| 10 | Adam Meyers | Senior Vice President | CrowdStrike |
| 11 | Niels van Ingen | Senior Vice President | Keepit |