11장. 최신 ICT 보안기술

박종혁

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech ac kr

개요

- **학습 목표**
  - ICT 및 최신 보안 기술에 대해 알아본다.
  - 최신 사이버 위협 사례와 동향을 분석하고, 10대 전략 기술 트렌드에 대해서 알아본다.

관련영상

- 주의를 기울이지 않으면 순식간에 당한다... 2024 보안 위협과 전망, 에티버스, 2024
  https://www.youtube.com/watch?v=xouVMOSAzIY

- 보안관제 자동화와 SOAR, IGLOO, 이규환 수석, eGISEC 2023 (배경 및 필요성 - 9:22까지 시청)
  https://www.youtube.com/watch?v=9PiP0q5MIlo

목 차

1. ICT 기술 / 보안

2. 최신 보안 기술
   - 인텔리전스 기반의 SOC 자동화
     - SOAR
   - 생성형 AI와 보안
   - IT-OT 융합 및 보안

3. 사이버 보안 위협 전망

4. 2025 10대 전략 기술 트렌드

1. ICT 기술/보안

- **ICT 기술**
  - ICT(Information and Communication Technology, 정보통신기술)은 정보와 통신 기술을 활용하여 정보를 생성, 저장, 처리, 전송, 공유, 활용하는 기술의 집합
  - 디지털 기술과 네트워크 기반 기술을 포함하여 광범위한 분야에 걸쳐 사용
  - ICT는 현대 사회에서 개인, 기업, 정부 등 다양한 주체의 의사소통 및 정보 활용 방식에 혁신을 가져옴
  - 사물인터넷, 클라우드, 블록체인, 양자통신 등 최신 정보기술을 활용하여 사물들이 데이터를 수집, 분석, 활용하고 이를 통해 인지, 학습, 추론과 같은 고차원적 정보처리 기능을 수행하도록 지능화되고있음

- # 최신 ICT 대표 기술

기술	개념
인공지능 (AI)	데이터를 학습해 문제 해결 및 의사결정을 지원하는 기술
빅데이터	대규모 데이터를 수집, 분석하여 유용한 정보를 추출하는 기술
클라우드 컴퓨팅	인터넷을 통해 데이터 저장 및 컴퓨팅 자원을 제공하는 기술
블록체인	데이터를 분산 저장하여 투명성과 보안을 강화하는 분산 원장 기술
5G 네트워크	초고속, 저지연, 대용량 데이터를 지원하는 차세대 이동통신 기술
사물인터넷 (IoT)	인터넷으로 연결된 기기 간 데이터 송수신 및 제어를 가능하게 하는 기술
엣지 컴퓨팅	데이터 처리를 장치 근처에서 실행해 지연을 최소화하는 기술
디지털 트윈	현실 세계의 물리적 객체를 가상으로 재현하여 시뮬레이션하는 기술
양자 컴퓨팅	양자역학 원리를 활용해 기존 컴퓨터보다 월등히 빠른 연산을 가능하게 함
사이버보안	정보와 시스템을 위협으로부터 보호하기 위한 기술 및 전략

기술	개념
증강현실 (AR)	현실 환경에 디지털 정보를 겹쳐 실시간으로 상호작용하는 기술
가상현실 (VR)	가상 세계를 시뮬레이션하여 몰입형 환경을 제공하는 기술
디지털 헬스케어	ICT를 활용하여 건강관리와 의료 서비스를 개선하는 기술
자율주행 기술	차량이 스스로 주변 환경을 인식하고 주행을 수행하는 기술
자연어 처리 (NLP)	인간 언어를 이해하고 처리하며 소통하는 인공지능 기술
로보틱스	정밀한 작업과 자율 작동이 가능한 로봇 개발 및 응용 기술
스마트시티	ICT로 도시 인프라를 효율화하고 지속 가능한 환경을 구현하는 기술
컴퓨터 비전	이미지와 영상을 분석하고 인식하는 인공지능 기술
지능형 엣지(AI Edge)	엣지 컴퓨팅과 AI를 결합해 빠른 데이터 분석과 처리를 가능케 하는 기술
무선충전 기술	전력을 케이블 없이 무선으로 전송하여 충전하는 기술

- **ICT 보안**
  - 목표: 데이터와 시스템의 안전성을 보장하기 위한 다양한 방법과 도구를 포함하며 일반적으로 기밀성, 무결성, 가용성을 확보
    - ✓ 암호화 기술, 방화벽, 침입 탐지 시스템, 보안 정보 및 이벤트 관리 시스템 등
  - 최근에는 인공지능과 빅데이터 기술을 활용한 보안 관제 시스템 및 위협 대응 자동화가 주목받고 있음
  - 양자 컴퓨팅 시대를 대비한 양자내성암호와 블록체인을 활용한 데이터 무결성 보장 기술도 점차 확대되고 있음

2. 최신 보안 기술

- 현대의 사이버 보안 환경은 점점 더 복잡해지고 있으며 지속적으로 진화하는 위협에 대응하기 위해 혁신적인 보안 기술의 도입이 필수적임

- 기존보안 시스템은 정적이고 단일 계층 방어에 의존
  - 오늘날 환경은 지능형 위협 분석 및 다계층 방어체계가 요구됨

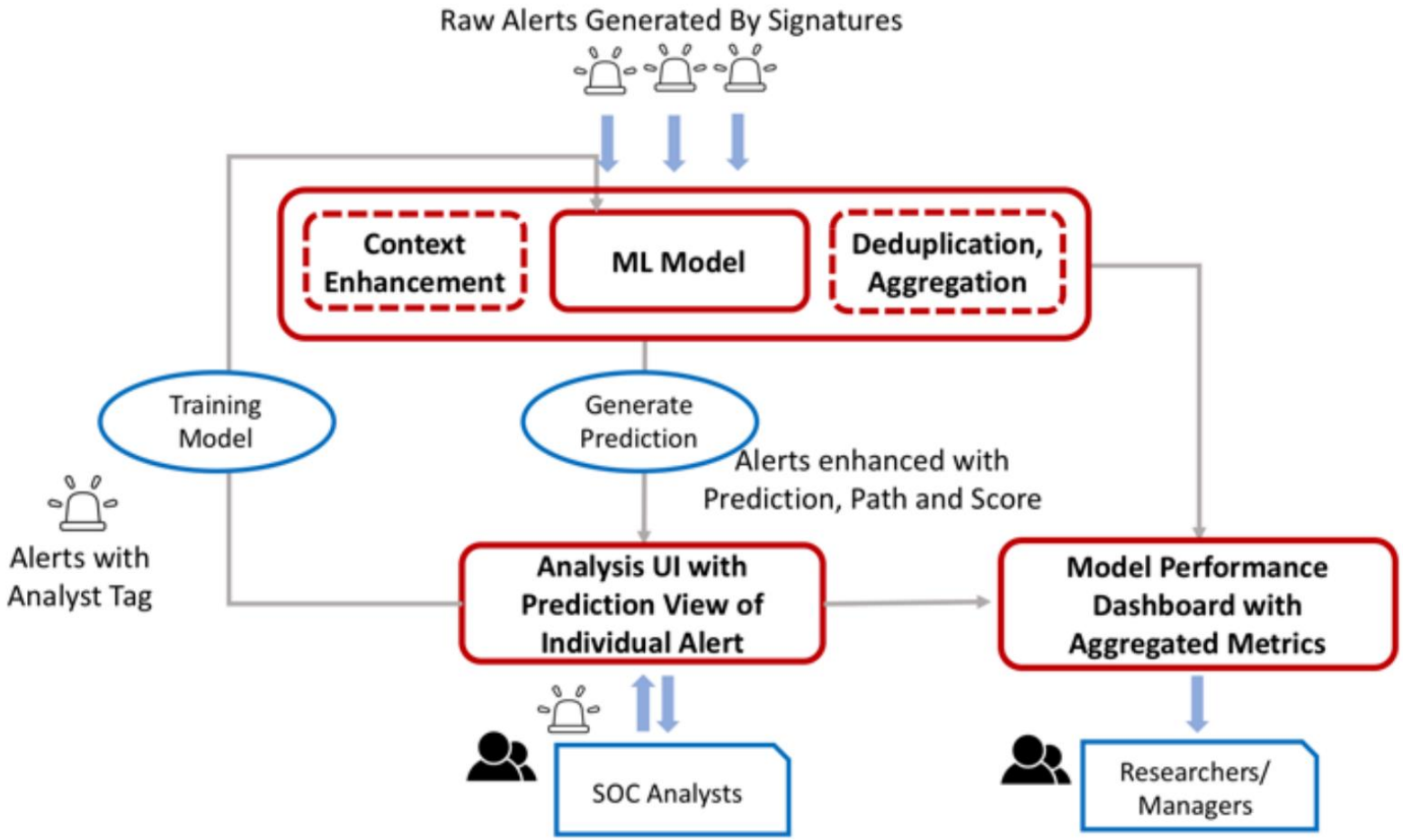
- 인공지능, 빅데이터, 클라우드 컴퓨팅 등 최신 ICT 기술을 활용한 새로운 보안 접근 방식이 주목받고 있음

2. 최신 보안 기술

- **인텔리전스 기반의 보안운영센터 (SOC, Security Operations Center) 자동화**
  - 고도화·지능화한 사이버 공격에 대응하기 위해 다양한 이기종 환경 전반에서 발생하는 로그나 이벤트를 인공지능, 빅데이터 등의 차세대 기술을 이용해 사이버 공격에 대응을 위한 보안관제센터가 필요
  - 생성형 AI와 오픈소스를 이용한 공격이 증가하는 상황에서 자동화된 보안 기술을 통해 보안 취약점을 관리하고 위협을 분석하며 가시성을 확보해 레질리언스를 강화함
  - 주요기능
    - ✓ 보안 이벤트 및 로그 모니터링
    - ✓ 위협 탐지 및 분석
    - ✓ 침해 사고 대응
    - ✓ 보안 경고의 우선순위 지정 및 관리
    - ✓ 인시던트 대응 자동화

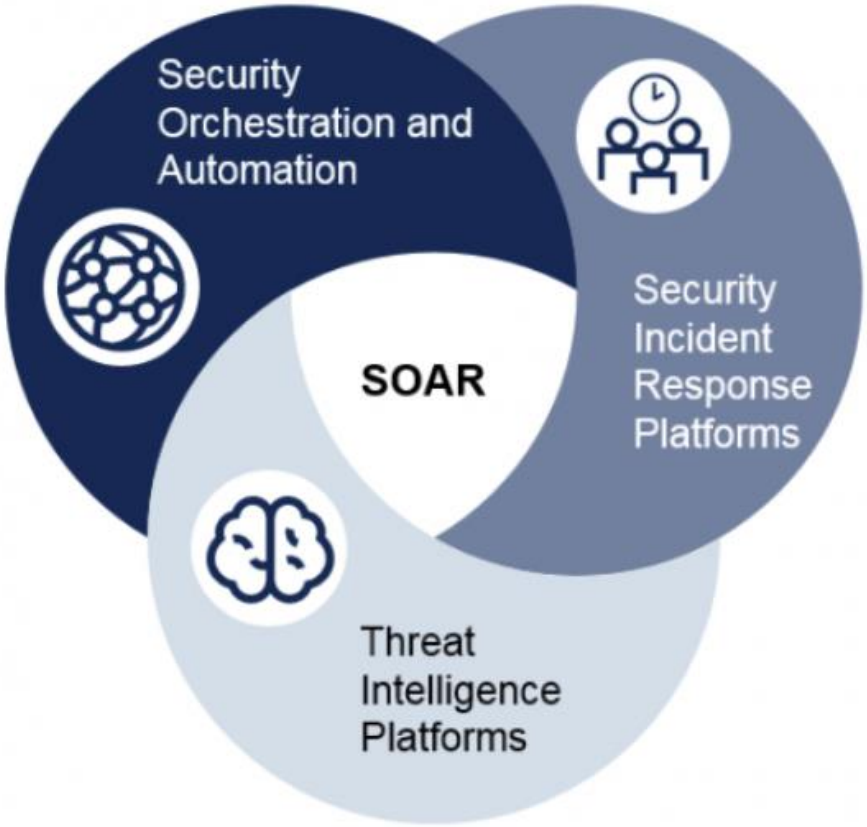
2. 최신 보안 기술

- 인공지능을 이용한 SOC 구성
  - 자동화된 보안관제의 보안 운영·위협 대응 자동화 (SOAR, Security Orchestration, Automation and Response) 분야에서 AI를 통한 지능화된 보안관제를 구성하는 연구가 진행



SOAR

- 보안 오케스트레이션, 자동화 및 대응(Security Orchestration, Automation, and Response)의 약자
- 보안 팀이 다양한 보안 도구와 프로세스를 통합하고 자동화하여 사이버 위협에 신속하고 효율적으로 대응할 수 있도록 지원하는 플랫폼



SOAR = SOA + SIR + TIP

- **SOAR 주요 구성 요소**
  - **보안 오케스트레이션**: 여러 보안 도구와 시스템을 연결하여 일관된 워크플로우를 구축
    - ✓ 보안 팀은 다양한 도구에서 발생하는 데이터를 중앙에서 관리하고 조율
  - **보안 자동화**: 반복적이고 시간이 많이 소요되는 작업을 자동화하여 보안 사고의 대응 속도를 높이고 인적 오류를 감소

    예) 위협 탐지 후 자동으로 방화벽 규칙을 업데이트하거나 의심스러운 IP를 차단하는 등의 작업이 포함
  - **보안 대응**: 수집된 정보와 자동화된 프로세스를 기반으로 신속하고 정확한 대응을 수행
    - ✓ 보안 사고의 영향을 최소화하고 복구 시간을 단축

- **SOAR 주요 기능**
  - 인시던트 관리: 보안 이벤트를 수집, 분류, 우선순위 지정하여 체계적으로 관리
  - 플레이북: 표준화된 대응 절차를 정의하여 일관된 대응을 보장
  - 위협 인텔리전스 통합: 최신 위협 정보를 통합하여 더욱 정확한 탐지와 대응을 지원
  - 보고 및 분석: 보안사고 대응 결과를 분석하고 보고서를 생성하여 보안 상태를 지속적으로 모니터링

- **SOAR 도입 효과**
  - 효율성 향상: 자동화를 통해 반복적인 작업을 줄여 보안 팀의 효율성 증가
  - 대응 시간 단축: 신속한 인시던트 탐지와 대응으로 피해를 최소화
  - 정확성 증대: 표준화된 프로세스를 통해 대응의 일관성과 정확성을 보장

생성형 AI와 보안

- **생성형 AI 개념**
  - 주어진 데이터를 학습하여 새로운 콘텐츠(텍스트, 이미지, 오디오, 비디오 등)를 생성할 수 있는 인공지능 기술
  - 기존 데이터를 분석하고 학습한 패턴을 기반으로 창의적이고 독창적인 결과물을 만들어내는 데 사용

- **주요 특징**
  - 데이터 생성: 새로운 텍스트, 이미지, 음악 등을 생성.
  - 패턴 학습: 기존 데이터의 패턴을 학습하여 이를 기반으로 콘텐츠를 생성
  - 다양한 응용 분야:
    - ✓ 텍스트 생성: ChatGPT, 블로그 작성, 코드 작성
    - ✓ 이미지 생성: DALL·E, 사진 및 디자인
    - ✓ 음악 및 영상 제작: AI 기반 작곡, 영상 편집

- **주요 기술**
  - 딥러닝, Transformer 모델 (GPT, BERT 등)

• 생성형 AI 기반 보안 응용

카테고리	내용 및 예시	활용 사례
자동 보안 위협 탐지 및 대응	악성코드 또는 피싱 이메일 패턴을 학습하여 미탐지된 위협을 탐지	GAN을 이용한 악성코드 탐지 시스템 강화
AI로 생성된 위협 시뮬레이션	공격 패턴을 예측 및 시뮬레이션하여 보안 테스트 강화	기업 네트워크의 취약점을 분석하고 공격 시나리오 생성
지능형 피싱 방어	피싱 이메일 패턴을 생성해 훈련 데이터셋 확장 및 감지 모델 개선	OpenAI 기반 텍스트 생성 모델로 피싱 이메일 시뮬레이션 훈련
정교한 인증 및 사용자 행동 모델링	정규 사용자 행동을 학습하여 비정상 행동 탐지 및 차단	OpenAI API를 활용한 비정상 로그인 패턴 식별
악성코드 생성 및 방어 시뮬레이션	다양한 형태의 악성코드를 생성하여 보안 소프트웨어의 내성 테스트	다형성 악성코드 시뮬레이션으로 보안 솔루션 반응성 개선
개인정보 보호 및 위협 제거	데이터에서 민감 정보를 자동으로 추출하고 가명화 처리	GPT 기반 모델로 데이터 처리 중 보안 강화

- **생성형 AI 기반 대표적 AI (보안) 프레임워크**

프레임워크 이름	개념 및 목표
AI TRiSM (Trust, Risk, Security Management) - 가트너	AI 모델의 거버넌스, 신뢰성, 공정성, 효율성, 개인정보보호, 데이터 보호 및 신뢰성 강화를 위한 방안 제시
시큐어 AI 프레임워크(SAIF, Secure AI Framework)	AI 시스템과 관련된 보안 메가 트렌드 및 위험에 대한 프레임워크로, 인공지능 소프트웨어 개발 공급망 검토, 테스트 및 제어를 포함한 보안 모범사례 제공
파운데이션 모델 투명성 지수(FMTI, The Foundation Model Transparency Index)	기초 모델 생태계의 투명성을 평가하고 향후 투명성 향상을 위한 지수 제공
FATE (Fairness, Accountability, Transparency, and Ethics in AI)	AI 연구와 개발의 공정성, 책임, 투명성, 윤리적 정의 및 연구를 목표로 하는 프레임워크
AI RMF (Artificial Intelligence Risk Management Framework) - NIST	AI 시스템 관련 부정적 영향을 최소화하고 긍정적 영향을 극대화하며, 기술에 대한 신뢰도를 높이기 위한 위험 관리 프레임워크
MITRE의 AI 보안을 위한 합리적인 규제 프레임워크	AI를 구성 요소로 사용하는 시스템, 사람의 능력 향상 AI, 자율적 운영 AI로 나누어 위협과 위험을 완화하는 3가지 범주로 보안 프레임워크 제시

– 세부내용

프레임워크	중점 사항	주요 내용
AI TRiSM	• AI Trust • AI Risk • SI Security Management	• 설명 가능성(Explainability), 모델운영(ModelOps), 데이터 이상 감지 (Data Anomaly Detection), 적대적 공격 방어(Adversarial Attack Resistance), 데이터 보호(Data Protection)
SAIF (Secure AI Framework)	• Stealing the model • Data poisoning of the training data • Injecting malicious inputs through prompt injection • Extracting confidential information in the training data	• AI ecosystem으로 강력한 보안 체계 구축 • 탐지 및 대응을 확장하여 조직 내 위협 탐지 AI 도입 • 기존 및 신규 위협에 대응하기 위한 방어 자동화(Automate defenses) • 플랫폼 수준 제어로 조직 전체에 일관된 보안 보장 • AI 배포를 위해 더 빠른 피드백 루프(faster feedback loops)를 생성 및 제어를 조정하고 완화 조치를 수행 • 비즈니스 프로세스상에서 AI 시스템 위험 컨텍스트화(Risk Contextualizing)
FMTI (The Foundation Model Transparency Index)	• The upstream / Downstream practices of the foundation model developer, Model-level 영역으로 투명성 개념 분석 • 모든 점수에 대한 이의 제기 기회 제공	• 회사 및 Foundation Model Developer를 대상으로 모델 개발 및 배포 투명성 평가 • 관련 규제 정책 계획 시 정보 활용 및 기업의 투명성 향상을 위한 동기 부여

프레임워크	중점 사항	주요 내용
FATE (Fairness, Accountability, Transparency, and Ethics in AI)	• 인공지능(AI)의 활용 증가로 인한 AI 프로그램의 도덕성 의문 제기	• FATE(공정성, 책임, 투명성, 윤리)와 AI에 대한 정의 및 사회적 영향 연구
AI RMF 1.0 (Artificial Intelligence Risk Management Framework)	• 유효성 및 신뢰성, 안전성, 보안 및 복원성, 책임과 투명성, 설명 및 해석 가능성, 개인정보 보호, 공정성	• 리스크 관리를 통해 시민의 자유와 권리 위협 등 AI 시스템의 잠재적인 부정적 영향을 최소화하고 긍정적인 영향 극대화
A Sensible Regulatory Framework for AI Security	• AI as a Subsystem • AI as Human Augmentation • AI with Agency	• AI 규제에 대한 잠재적 사항과 AI 개발 및 사용을 위한 가이드라인 설정에 대한 권장 사항 제시

IT-OT 융합 및 보안

- IT-OT 융합
  - IT (Information Technology)와 OT (Operational Technology) 융합은 디지털 혁신의 중요한 축
  - -IT는 데이터를 수집, 저장, 처리, 분석하는 기술이며, OT는 물리적 프로세스 및 시스템을 모니터링하고 제어하는 기술

- IT-OT 융합 생태계는 제조, 에너지, 헬스케어, 물류 등 다양한 산업에 활용
  - 데이터 통합: OT에서 생성된 데이터를 IT로 가져와 분석 및 시각화
  - 효율성 향상: OT 프로세스를 IT 분석을 통해 최적화
  - 실시간 제어 및 의사결정: IoT 센서 및 엣지 컴퓨팅 기술을 통해 OT 시스템의 실시간 모니터링
  - 스마트 팩토리 구현: 디지털 트윈, 예지보전, 자율 생산 시스템 등 첨단 기술 적용

- IT-OT 융합 보안
  - IT-OT 융합 보안은 IT와 OT가 연결된 환경에서 발생하는 사이버 위협과 물리적 위협을 식별하고, 이를 예방하거나 완화하는 보안 전략 및 기술
  - 디지털 혁신 과정에서 필수적인 영역으로, IT 시스템의 데이터 보안 요구와 OT 시스템의 물리적 안정성을 동시에 보장해야함

- IT-OT 보안의 차이점 및 중요점

항목	IT 보안	OT 보안
목적	데이터의 기밀성, 무결성, 가용성	시스템의 가용성 및 안전성
운영 우선순위	시스템 중단 시 데이터를 보호	시스템 중단 방지(안정적 운영)
위협 요소	데이터 유출, 무단 접근	물리적 사고, 생산 차질, 인명 피해
취약점	네트워크, 소프트웨어	오래된 하드웨어, 폐쇄망 환경

  - IT-OT의 융합으로 두 영역의 보안 요구사항이 교차하며 새로운 위협이 등장 가능

- **IT-OT 융합 보안의 주요 구성 요소**
  - **통합 네트워크 보안**
    - ✓ IT-OT 네트워크 간 경계 보호 및 위협 탐지
    - ✓ 방화벽, IDS/IPS와 같은 네트워크 보안 솔루션 도입
  - **접근 제어 및 인증**
    - ✓ 최소 권한 접근 제어(RBAC) 및 다중 인증(MFA) 활용
    - ✓ 무단 접근 방지를 위한 인증 시스템 구축
  - **위협 탐지 및 대응**
    - ✓ SIEM 및 SOAR를 통한 실시간 위협 모니터링
    - ✓ 자동화된 대응 체계로 위협 처리 시간 단축

* SIEM: IT 시스템의 로그와 이벤트 데이터를 수집, 분석하여 보안 위협을 실시간으로 탐지하고 대응하는 통합 솔루션

- **자산 및 취약점 관리**
  - ✓IT 및 OT 자산 식별 및 정기적 관리
  - ✓취약점 평가 도구를 사용하여 보안 위험 완화

- **보안 정책 및 거버넌스**
  - ✓IT-OT 통합 보안 정책 수립 및 규제 준수 관리
  - ✓보안 프레임워크(NIST, IEC 62443 등) 기반 거버넌스 구축

- **교육 및 인식 제고**
  - ✓사용자 및 관리자 대상 보안 훈련 프로그램 제공
  - ✓IT-OT 협력을 위한 시나리오 기반 교육 시행

- **디지털 전환을 통한 IT-OT 융합생태계 구축**
  - 스마트 시티: 도시가 제공하는 교통, 안전, 생활 등의 편의성을 증대하기 위한 목적성을 띰
    - ✓ 스마트 그리드를 결합하여 지능형 전력 수요 관리, 신재생 에너지 연계, 운영 효율화
    - ✓ 전력망 감시·보호의 고도화 및 전기차 운행 인프라 기술 등을 결합하여 편의성과 효율성을 제공
  - 운송 분야: 운송 수단이 무인화될 수 있는 자율 운행 자동차, 자율 운항 선박, 도심항공교통 등에 적용
    - ✓ 자율 운항 선박의 경우: 육상에서 선박을 원격으로 조종해 선박 내 시스템을 감독 ·관리 및 시스템 문제 제어
    - ✓ 최적의 항로를 인공지능으로 분석하는 형태로 기술 활용

- **IT-OT 융합 보안: CPS 보안 중심**

관점	세부기준	발생 가능한 위협	대응방안
CPS 보안을 위협하는 환경요소	물리적 환경요소	• 물리적 장치 변조로 인한 가용성 상실 • 천재지변 : 홍수, 태풍, 지진 등	• 버튼, 포트, 케이블, 네트워크 연결, 전원 등 장치의 물리적 변조 방지 필요 • MIL-STD-810(Military Standard Environmental Engineering Considerations and Laboratory Tests) 표준 규격(온도, 습기, 모래/먼지, 부식 등 적합성 검토)에 맞는 장치 고려
	운영 환경요소	• 운영 실수 : 운영 미숙, 교육 부족, 운영 절차 위반 등 • 가용성 훼손 시 대책 미흡 : BCP, DRS 등 • 부적절한 패치 관리	• 표준 운영 절차 및 계획 수립, 장치에 대한 운영 백업 계획, 중단 계획, 공격 시 예외 처리 기능 필요 • 계획되지 않은 재부팅의 허용 금지 등, 전원 오류, 재해 복구 및 고가용성에 대한 고려 필요 • 시스템 모든 구성 요소에 대한 지원 가능성 • 물리적 장치에 대한 부품 및 소프트웨어 업그레이드 및 보안 패치에 대한 정책 수립 필요
	사회·경제적 환경요소	• 과도한 개발 비용 증가 • 사람과 상호 작용 미흡(운영의 편리성 등) • 안전성 미흡	• 개방형 참조 아키텍처 및 표준, 모델 기반 엔지니어링 방법론, 시뮬레이션, 검증 및 검증 도구 개선을 통해 개발 비용 절감 • 사람과 기술, 복잡한 인프라와 인간 간의 상호 작용 활용, 경제적, 사회적, 환경적 방식으로 이해관계자의 요구, 욕구 및 열망 충족 관점에서 접근 필요 • 안전성, 신뢰성 향상 및 가치 향상을 통해 투자 수익 입증

관점	세부기준	발생 가능한 위협	대응방안
CPS보안을 위협하는 서비스 요소	개인정보	• 개인정보 관리 미흡 및 유출	• 개인 정보의 보호, 강화, 민감한 개인 정보의 적절한 사용을 위한 CPS 기술 및 기법 필요 • 지리적 위치 및 해당 국가 법률에 따른 암호화, 저장 등 개인 정보 보호 전략 필요
	운영 계층 간 상호 작용	• 기존 보안 솔루션 호환성 문제 • 물리 시스템에서 사용되는 네트워크의 암호화 미흡	• 개별 CPS를 시스템을 안정적이고 검증 가능하게 조립할 수 있는 모듈화 및 구성에 대한 접근 방식 필요 • 각 운영 계층에 대한 위험 평가를 통한 잠재적인 영향과 완화 전략 수립 필요
CPS 보안위협의 대응기술요소	사이버 보안	• 운영 체제 또는 응용 프로그램의 결함 • 악성코드, 랜섬웨어 • 공급망 공격	• 네트워크로 연결된 사이버 물리 시스템과 중요 인프라의 사이버 공격에 대한 탄력성(resilient) 중요 • 운영 체제 또는 응용 프로그램의 결함으로 인한 위협에 의해 침투 테스트, 취약점 점검, 패치 관리 필요

- **IT-OT 융합 보안: 클라우드 보안 중심**

측면	프레임워크	설명	보안 정책 예시
Cloud 측면	CNAPP (Cloud Native Application Protection Platform)	• 개발 및 프로세스 전반에 걸쳐 클라우드 네이티브 애플리케이션을 보호하고, 보안을 강화하도록 설계된 보안 및 컴플라이언스의 통합 세트 정의	• 아티팩트 스캐닝(Artifact scanning), 코드형 인프라(IaC : Infrastructure as Code) 스캐닝 가능 • CIEM, CSPM, CWPP 통합
	CASB (Cloud Access Security Broker)	• 클라우드 기반 리소스에 액세스할 때 엔터프라이즈 보안 정책을 결합하고 삽입하기 위해 클라우드 서비스 소비자와 클라우드 서비스 공급자 사이에 배치되는 온프레미스 또는 클라우드 기반 보안 정책 적용 지점 • 여러 유형의 보안 정책 시행을 통합	• 인증, SSO(Single Sign-On), 권한 부여, 자격 증명 매핑, 장치 프로파일링, 암호화, 토큰화, 로깅, 경로, 멀웨어 탐지/방지 등
	CWPP (Cloud Workload Protection Platforms)	• 클라우드 서버워크로드 중심의 보안을 위한 솔루션, 워크로드에 대한 가시성 확보 및 공격 방어가 목적	• 시스템 무결성 보호, 마이크로 세그먼트, 메모리 보호, 사용자 행동 모니터링, 호스트 기반 침입 방지 및 멀웨어 방지
	CSPM (Cloud Security Posture Management)	• 공격 성공 가능성을 줄이기 위한 지속적인 클라우드 보안 개선 및 적응 프로세스	• 클라우드 구성 오류 감지 및 자동 수정
	CIEM (Cloud Infrastructure Entitlement Management)	• 하이브리드 및 멀티클라우드 Iaas의 권한 거버넌스를 위한 관리 시간 제어를 통해 클라우드 액세스 위험을 관리하는 데 초점을 맞춘 전문 ID 중심 SaaS 솔루션	• 리소스 프로비저닝/관리 기능 • 사용량 모니터링/감사 기능

측면	프레임워크	설명	보안 정책 예시
인프라 측면	KSPM (Kubernetes Security Posture Management)	• 자동화 도구를 활용하여 모든 Kubernetes 구성 요소에서 보안, 잘못된 구성 및 규정 준수 문제 식별 및 해결	• RBAC(역할 기반 액세스 제어) 문제 식별, 네트워크 보안 정책 편차 감지, HIPAA, SOX, ISO/IEC 27001과 같은 표준 준수, 문제 발생 시 자동 대응 또는 수정 단계 제안
	SSPM (Software-as-a-Service Security Posture Management)	• 조직의 가시성 확보 및 SaaS 환경의 보안 상태 관리 도구	• 데이터 모니터링 및 분석, SaaS 애플리케이션 내 잘못된 구성 및 과도한 권한 등 취약성 식별, 다단계 인증 및 암호화와 같은 보안 제어, 위험 식별 및 우선순위 지정, 데이터 보호 및 개인 정보 보호법과 같은 규정 및 표준 준수 확인
	SSE (Security Service Edge)	• 클라우드 기반 서비스를 통해 사용자에게 보안 연결 제공, 클라우드 기반 서비스를 위해 사용자를 기업 네트워크에 직접 연결할 필요 없음	• CASB, ZTNA, SWG, FWaaS(Firewall-as-a-Service)기능 구성
APP 측면	WAAP (Web Application and API Protection)	• 클라우드 WAAP는 주로 공용 웹 애플리케이션 및 API를 보호하는 클라우드 제공 서비스	• 런타임 공격, 웹 애플리케이션 위협, 자동화된 위협, API에 대한 특수 공격에 대한 OWASP 상위 10대 공격 완화
	SWG (Secure Web Gateway)	• 웹/인터넷 트래픽에서 원치 않는 소프트웨어/악성 프로그램을 필터링하고 기업 및 규정 정책 준수 시행	• URL 필터링, 악성 코드 탐지 및 필터링, IM(instant messaging) 및 Skype와 같은 웹 기반 애플리케이션 제어 기능
	ZTNA (Zero Trust Network Access)	• 애플리케이션 또는 애플리케이션 세트 주위에 ID 및 컨텍스트 기반의 논리적 액세스 경계 생성	• ID 기반 액세스 제한, SASE(Secure Access Service Edge) 통합을 통해 원격 액세스 보안, 모니터링을 통한 데이터 손실, 사용자 자격 증명 손상 방지

3. 사이버 보안 위협 전망

- **피해 자체를 모르게 하는 은밀하고 지속적인 SW 공급망 공격**
  - 해킹 그룹은 인터넷에 무상으로 공개된 소스 코드나 SW들을 프로그램 개발자들이 많이 이용하는 것을 악용
    - ✓ 유명한 오픈소스를 사칭하거나 변조된 코드를 배포해 개발자 대상 공격을 확대
  - 개발자 시스템을 장악 : APT을 통해 은밀히 침투하여 개발 제품에 악의적인 코드를 쉽게 포함시킴
  - SW 공급망을 통한 공격 시도도 증가하여 악성코드 배포
    - ✓ SW 이용기업이나 기관들은 악성코드 등이 침투되었다는 사실을 인지하지 못하고 고객사 등 다른 이용자에게 연쇄적인 피해를 줌

- **생성형 AI를 이용한 사이버 범죄 증가**
  - 챗GPT를 화두로 생성형 인공지능 기술의 급속한 발전으로 이해 사용자가 보안에 대한 전문적인 지식이 없더라도 손쉽게 악성코드 제작 가능
  - 취약점 확인, 사회 공학적 공격, 음성 위변조 등 다양한 사이버 공격에 악용될 수 있는 위험성 내포
  - 생성형 AI 및 AI 대규모 언어모델을 활용하여 범죄 대상과 범죄 방법을 제공하는 서비스가 다크웹 등 해킹 포럼에 소개
    - ✓ 누구나 쉽게 사이버 범죄에 가담
  - 공격자가 기술 용어나 특정 비즈니스 영역에 능통하지 않더라도 공격 대상이 쉽게 속을 수 있도록 정교하게 이메일 작성 및 악성프로그램 제작
    - ✓ 피싱 이메일 공격을 도와주는 생성형 AI 기반의 사이버 범죄 도구가 최근 발견됨

- **OT/ICS 및 IoT 환경의 보안 위협 증가**
  - 스마트 설비와 디지털 트윈등 IT기술이 현장에 적용 되면서 OT, 산업 제어시스템(ICS: Industrial Control System), IoT 기반 시스템과 상호 간에 연결이 증가하여 보안 위협도 함께 급증
  - 최근 글로벌 보안업체 발표에 따르면 전세계 ICS 중 33% 이상에서 악성코드가 탐지 (이중 10%는 지속적으로 감염이 반복)
  - OT/ICS 환경은 일반적으로 IT 환경보다 기능이 제한적이지만 취약점에 대한 펌웨어 등 보안패치가 제조사별로 늦게 제공되거나 서비스 무중단을 이유로 <u>소극적으로 보안패치 적용을 하는 등 문제점</u>이 있음

- **정치·사회적 이슈를 악용하는 사이버 위협 고조**
  - 국가적인 중요한 행사가 있을 때 사회혼란을 노리는 세력들의 사이버 위협가능성도 함께 증가
  - 해킹그룹은 목표물을 공격하기위한 사전작업으로 목표관계자와 주변을 SNS로 확인
    - ✓ 피싱공격, 악성코드 감염, 해킹 등을 통해 얻은 시스템 관리자 등의 계정정보를 이용
  - 딥페이크기술을 적극 활용해 가짜뉴스를 생산하고, 예전에 유출된 내용으로 거짓해킹을 주장
  - 핵티비스트(Hacktivist: Hacking+activist)들은 자신들의 신념에 따라 공격 대상을 정해 지속적인 공격을 진행
    - ✓ 핵티비스트: 주로 정부, 기업, 단체의 정보 시스템에 침입하거나 데이터를 노출시키며 자신들의 메시지를 전달하거나 항의를 표현

      . 수단: DDoS 공격, 데이터 유출, 웹사이트 변조 등

4. 2025 10대 전략 기술 트렌드 (가트너)

2025 Top 10 Strategic Technology Trends

AI imperatives and risks
- Agentic AI
- AI Governance Platforms
- Disinformation Security

New frontiers of computing
- Post-Quantum Cryptography
- Ambient Invisible Intelligence
- Energy-Efficient Computing
- Hybrid Computing

Human-machine synergy
- Spatial Computing
- Polyfunctional Robots
- Neurological Enhancement

Source: Gartner
© 2024 Gartner, Inc. and/or its affiliates.
All rights reserved. 3185862

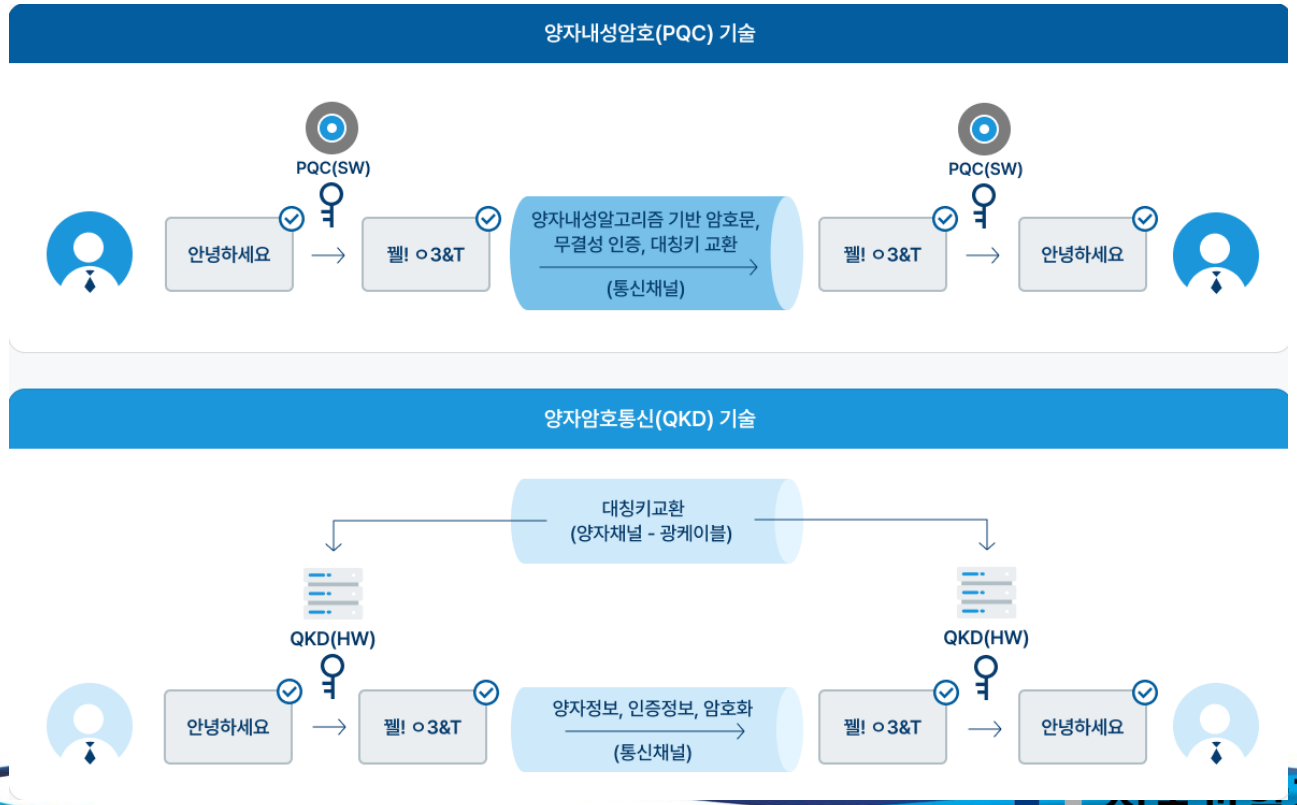
Gartner

- **에이전틱 AI (Agentic AI)**
  - 자율적인 의사결정 기능을 갖추고 특정 목표를 달성하기 위해 독립적으로 행동할 수 있는 시스템
  - 사용자가 정의한 목표를 달성하기 위해 자율적으로 계획하고 실행하며 인간의 업무 부담을 완화하고 보강할 수 있는 가상 인력의 가능성을 제시
  - 다양한 작업을 처리할 수 있는 보다 적응력 있는 소프트웨어 시스템 제공
  - 인간처럼 자체적으로 계획을 세워 목표를 달성하는 데 큰 차이가 있으며 향후 AI 어시스턴트에 통합되어 소프트웨어, SaaS 플랫폼, IoT 디바이스, 로봇 공학에 내장될 것으로 예측됨

- **AI 거버넌스 플랫폼 (AI Gorvenance Platforms)**
  - AI 시스템의 개발, 배포, 운영을 관리하고 모니터링하는 종합적인 프레임워크와 도구를 제공하는 플랫폼
  - 진화하는 AI 신뢰, 위험 및 보안 관리(TRiSM) 프레임워크의 일부이며 기업이 AI 시스템의 법적, 윤리적, 운영적 성과를 관리하도록 지원
  - 책임감 있는 AI 사용을 위한 정책을 수립, 관리, 시행하고 AI 시스템의 작동 방식 설명 및 투명성을 제공해 신뢰와 책임감을 구축
  - AI 관련 윤리적 사고를 방지할 수 있으며 AI 서비스의 신뢰성, 투명성, 공정성, 책임성을 보장하여 AI가 보다 안전하고 윤리적으로 사용되게 함

- **허위 정보 보안 (Disinformation Security)**
  - 인공지능 및 고급 분석 기술을 활용하여 가짜 뉴스, 딥페이크 등의 허위정보를 탐지하고 방지하는 보안 시스템
  - 신뢰할 수 있는 정보를 체계적으로 식별하고 무결성 보장, 진위 여부 평가, 사칭 방지, 유해 정보 확산 추적을 위한 방법론적 시스템을 제공하는 새로운 기술 범주
  - 허위 정보 보안 사용 사례를 해결하는데 특화된 제품, 서비스, 기능을 도입하는 기업이 현재의 5% 미만에서 2028까지 50%로 증가할 것으로 예측

- **양자내성암호 (Postquantum Cryptography, PQC)**
  - 양자컴퓨터의 공격에도 안전한 새로운 암호화 알고리즘 및 프로토콜을 개발하고 구현하는 기술
  - 양자 컴퓨팅 복호화 위험으로부터 데이터를 보호하며 지난 몇 년 동안 양자 컴퓨팅이 발전하면서, 널리 사용되는 많은 유형의 기존 암호화 방식이 더 이상 유효하지 않게 될 것으로 예상



- **앰비언트 인비저블 인텔리전스 (Ambient Invisible Intelligence)**
  - 일상 환경에 자연스럽게 통합되어 사용자의 요구를 예측하고 지원하는 보이지 않는 형태의 인공지능 기술
  - 초저가의 소형 스마트 태그와 센서를 통해 저렴한 비용으로 대규모 추적 및 감지를 가능하게 함
  - 사용자에게 거의 인식되지 않지만, 환경의 모든 변화를 실시간으로 감지할 수 있어 장기적으로 일상생활에 센싱과 인텔리전스의 더 깊은 통합을 끌어낼 것으로 예상

- **에너지 효율적 컴퓨팅 (Energy-Efficient Computing)**
  - 컴퓨터 성능을 유지하거나 향상시키면서 에너지 소비를 최소화하는 하드웨어 및 소프트웨어 기술
  - 2020년대 후반부터 AI 및 최적화와 같은 특수 목적의 작업을 위해 광학, 뉴로모픽(Neuromorphic), 새로운 가속기 등 새로운 컴퓨팅 기술이 등장할 것이며, 이는 훨씬 적은 에너지를 사용하게 됨

- **하이브리드 컴퓨팅 (Hybrid Computing)**
  - 전통적인 컴퓨팅 시스템 및 양자 컴퓨팅, 신경망 컴퓨팅 등 새로운 패러다임을 결합한 혁신적인 컴퓨팅 아키텍처
  - 다양한 컴퓨팅, 스토리지, 네트워크 메커니즘을 결합하여 계산 문제를 해결하며 기업이 문제를 탐색하고 해결하여 AI와 같은 기술이 현재의 기술적 한계를 뛰어넘는 성능을 발휘
  - 중앙처리장치(CPU), 그래픽처리장치(GPU), 에지, 주문형 반도체, 고전 양자, 광학 컴퓨팅 등 새로운 컴퓨팅 패러다임이 지속적으로 등장

- **공간 컴퓨팅 (Spatial Computing)**
  - 물리적 공간과 디지털 정보를 융합하여 사용자에게 몰입형 상호작용 경험을 제공하는 기술
  - 물리적 환경과 가상 환경 간의 상호작용을 한 차원 높여주며, 향후 5~7년 내에 간소화된 워크플로우와 향상된 협업을 통해 기업의 효율성을 높임

- **다기능 로봇 (Polyfunctional Robots)**
  - 다양한 작업과 환경에 적응할 수 있는 유연성과 다기능성을 갖춘 로봇 시스템
  - 두 개 이상 작업을 수행할 수 있는 기능을 갖추고 있으며, 단일 작업을 반복적으로 수행하도록 맞춤 설계된 작업 전용 로봇을 대체
  - 새로운 로봇은 효율성을 개선하고 더 빠른 ROI를 제공하며, 인간과 협업할 수 있게 설계돼 빠른 배치와 손쉬운 확장이 가능
- **신경학적 향상 (Neurological Enhancement)**
  - 인간의 인증 능력과 신경계 기능을 향상시키기 위한 기술적, 의학적 접근법
  - 인지 능력을 강화하고, 브랜드가 소비자의 생각과 감정을 파악할 수 있게 하고, 인간의 신경 능력을 향상시켜 최적의 결과물을 도출

참고문헌

- 2024년 ICT 10대 이슈, IITP, 2024
- What is SOAR?, IaSalle Blogging, 2024
- SOAR(보안 오케스트레이션, 자동화 및 대응)이란 무엇인가요?, IBM, 2024
- SOAR이란?, Palo Alto Networks, 2024
- ICT융합보안의 이해, 진한엠앤비, 2020
- 2024년 사이버 보안 위협 분석 과 전망, KISA, 2024
- 2024년 사이버 보안 위협 및 기술 전망, IGLOO, 2024
- 디지털 비즈온, 가트너 2025년 10대 전략 기술 트렌드 발표, 2024
- 최신 ICT 대표 기술 등, Chat GPT, 2024