Cyber Security Conference 2021

SAMSUNG SDS

스마트팩토리 시대의

삼성SDS OT보안 방안

성장환 프로 삼성SDS 보안플랫폼팀

AGENDA

Ⅰ. 스마트팩토리 보안 현황

Ⅱ. OT 보안 방안

Ⅲ. 삼성SDS의 OT보안 관제 소개

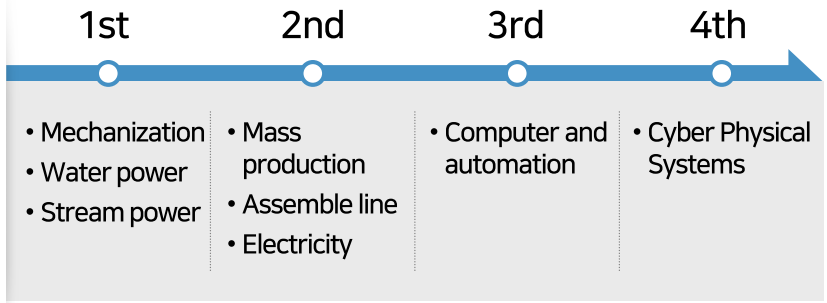
스마트팩토리란?

스마트팩토리 정의

설계 및 개발, 제조 및 유통 등 생산 과정에

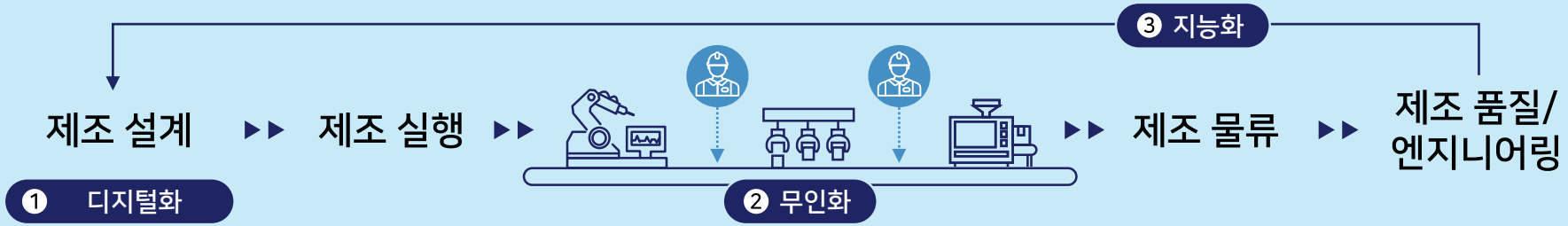
- 디지털 자동화 솔루션이 결합된 정보통신기술(ICT)를 적용하여
- 생산성, 품질, 고객만족도를 향상시키는 지능형 생산공장으로
- 공장 내 설비와 기계에 사물인터넷(IoT)을 설치하여

공정 데이터를 실시간으로 수집하고, 이를 분석해 스스로 제어되는 공장

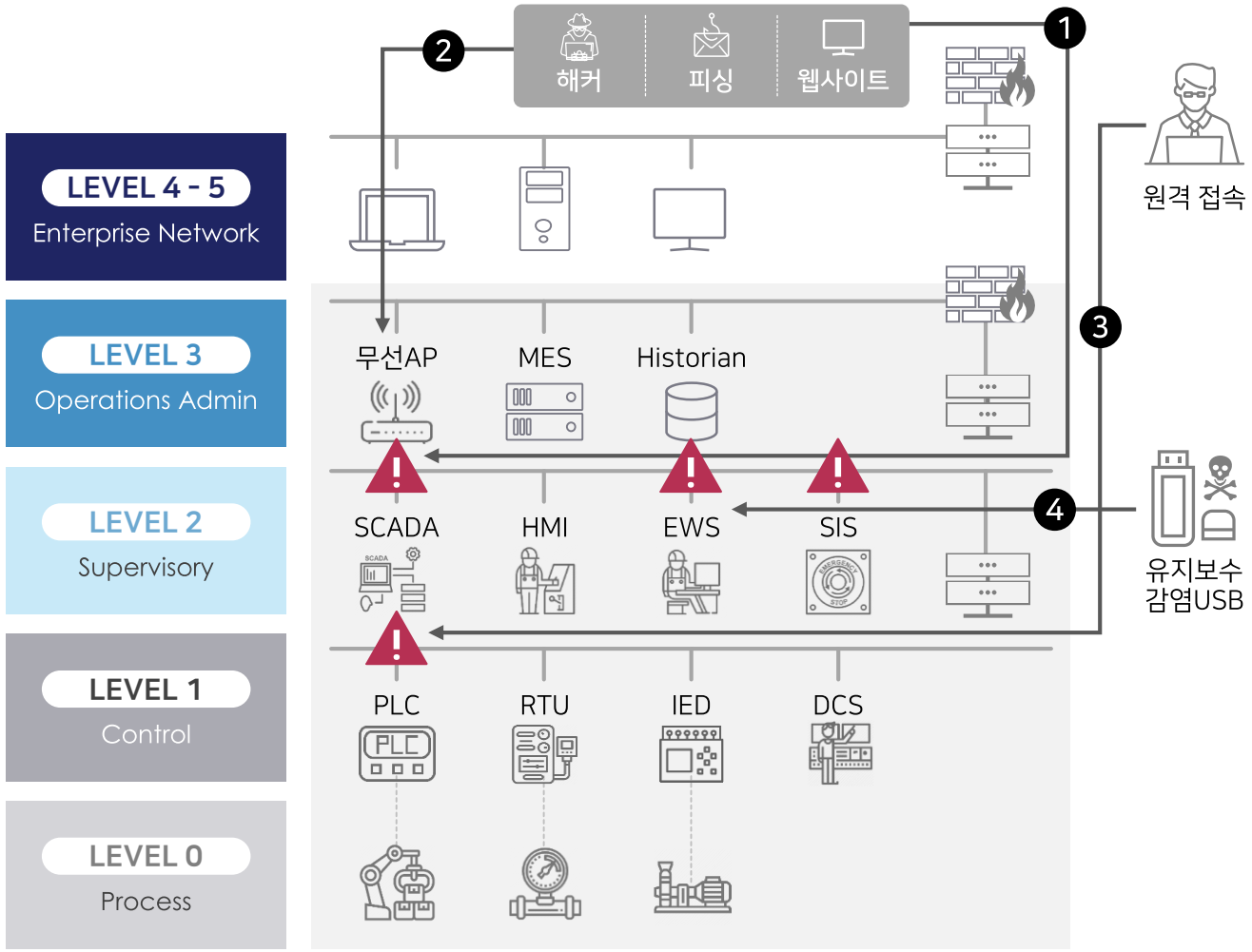


스마트팩토리 사례

- 제조설계, 생산, 물류, 품질분석 등 제조 全 프로세스 연계 데이터 수집/분석/예측 기능 강화로 실시간 종합 관제 체계 구축
- Rule과 프로세스 반영하고 Data를 분석하여 의사결정 지원이 가능한 인공지능 수준의 시스템 구축



OT보안 위협 경로



위협 경로

1. 웹사이트에 접속하여 악성코드에 감염된 IT망에서 OT망으로 전파
   악성코드에 감염된 내부 운영자PC에서 OT망 내부로 원격접속
2. 보안 설정에 취약한 무선AP를 경유한 외부 비인가자에 의한 OT망 무단침입
3. 외부 인터넷에 오픈된 원격접속 경로를 통한 악성코드 감염
4. 유지보수 업체 엔지니어를 통해 반입된 PC / USB에 저장된 악성코드 유입

고객 현안

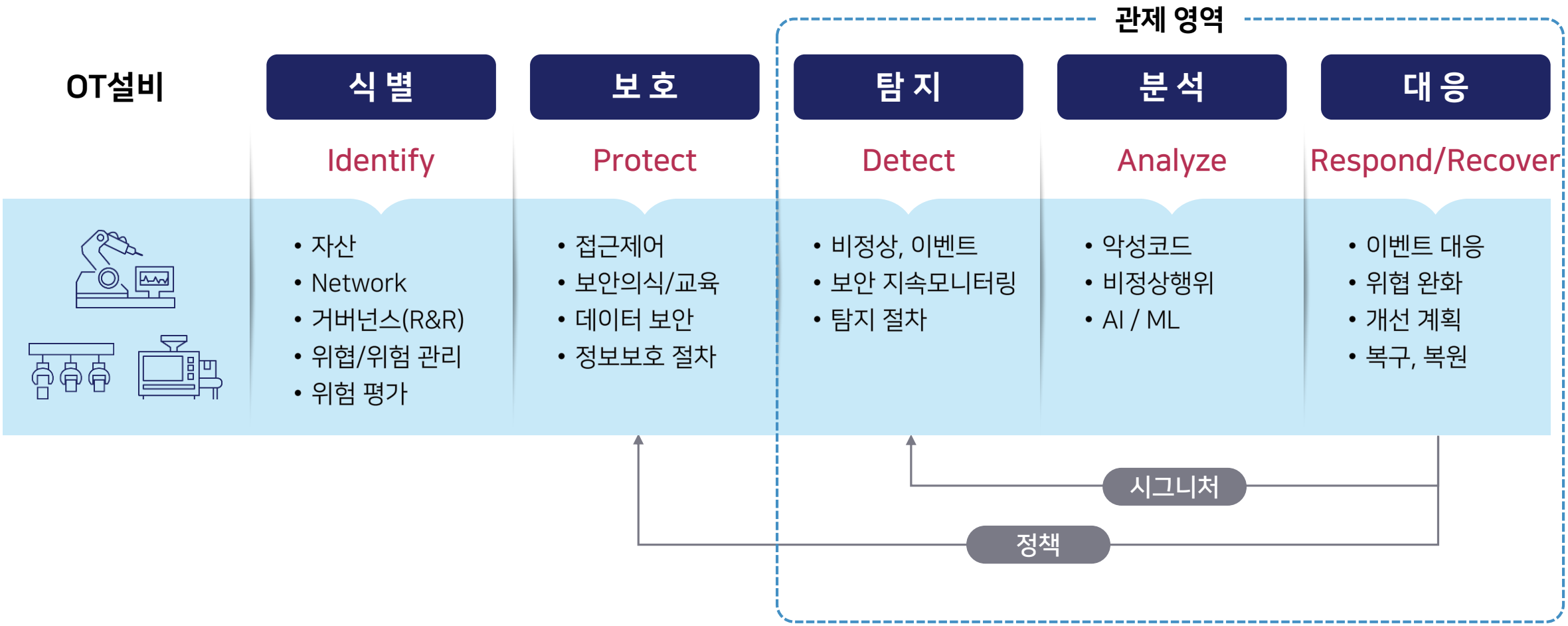
다수의 제조/생산 기업은 IT망과 OT망을 Firewall를 적용하여 이미 분리된 폐쇄망으로 운영중이라 위협요소가 없는 안전한 환경이라는 인식이 많으나, 실제 현장상황을 분석하면 많은 보안 Risk가 존재함

현실 대응 현황 (문제점)

- 네트워크, OT자산 현황을 모르겠다.
  → 가시성 미흡으로 현황파악 및 대응 어려움
- Endpoint 관리가 힘들다.
  (Patch, ID/PASSWD, USB관리 등)
- 현장에 보안전문가가 없다.
  (품질, 생산성이 우선, 보안 가이드도 없고..)
- FW는 설치했는데, 제대로 관리되고 있는 건지…
  → Network Segmentation 부재로 확산 우려
- OT보안은 어느 조직에서 담당하지?
  (공장 보안 Ownership 부재)

삼성SDS OT보안 모델

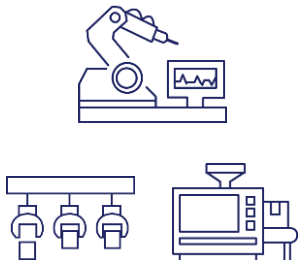
삼성SDS는 OT 자산(설비)를 식별/보호하고 위협을 탐지하여 전문가가 분석 대응하는 순환적 모델을 보유



삼성SDS OT보안 모델

삼성SDS는 OT 자산(설비)를 식별/보호하고 위협을 탐지하여 전문가가 분석 대응하는 순환적 모델을 보유

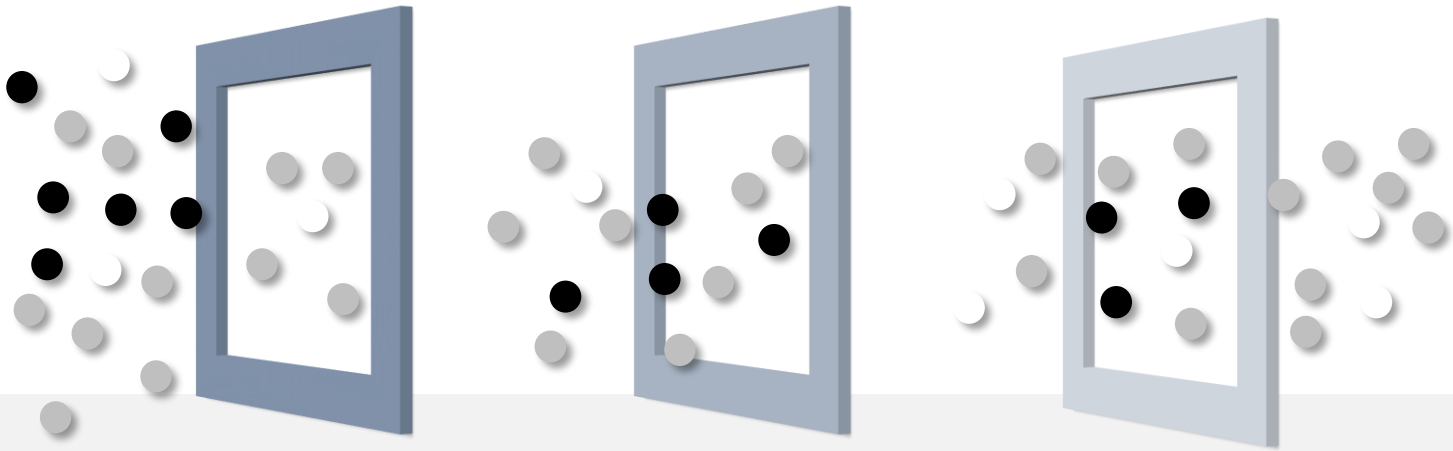
관제 영역

	OT설비	Identify	Protect	Detect	Analyze	Respond
Solution		OT 가시화 및 위협 탐지(DarkTrace IIS, Claroty, NOZOMI)				
		Endpoint(Nexplant OT Viewer, XGuard)				
			Network Seg(BLUEMAX)			
		인증(EAMS)				
				보안 운영 효율화 솔루션 및 서비스(AMAS, SNOW, FPMS)		
Service		보안 컨설팅 및 시스템 구축		보안 관제		
		• OT 보안 조직/전략 • 위협, 위험 분석 • 취약점 진단, 모의 해킹 • 보안 정책, 로드맵 수립	• 보안 아키텍처 설계 • 솔루션 Implementation • OT-IT Governances 수립	• 비정상 이벤트 • 보안 지속모니터링 • 탐지 절차 자동화	• 포렌식 기반 악성코드 • AI/ML 기반 이상행위탐지 • 위협 대응, 위협 완화 • 보안 위협 개선, 복구	

AI기반 위협 탐지 – Darktrace IIS(Industrial immune System)

OT보안 사고 방지를 위해서는 차단/방어 중심에서 예방/분석 중심으로 변화가 필요

기존 OT보안솔루션의 한계



방화벽/망분리
- IP/Port 차단/허용

IPS
- 패턴기반의 공격차단

VirusWall/백신
- 시그니처기반 차단
- 특정 OS에 설치
- 특정 실행파일만 동작

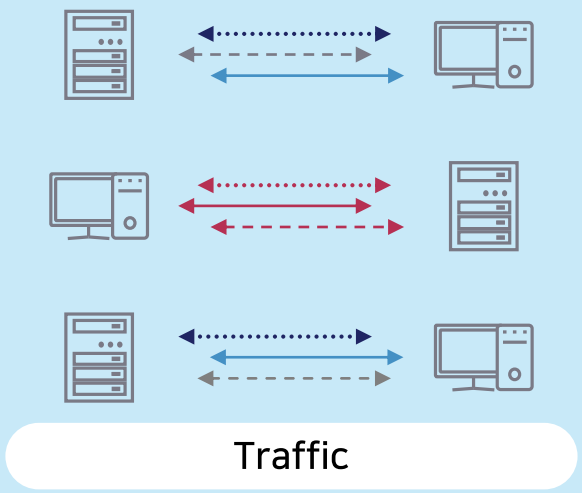
Black List	차단 중심
Gray List 데이터 증가에 따른 영역 확대	**전수검사 필요** ▸▸▸ 대상의 방대성
	분석의 효율성
White List	허용 중심

AI기반 위협 탐지 – Darktrace IIS

Dark Trace는 Network Traffic 기반으로 사용자, 디바이스, 네트워크 행위의 방대한 정보를 수집, 학습/추론, 시각화를 통해 실시간 보안 가시성을 확보

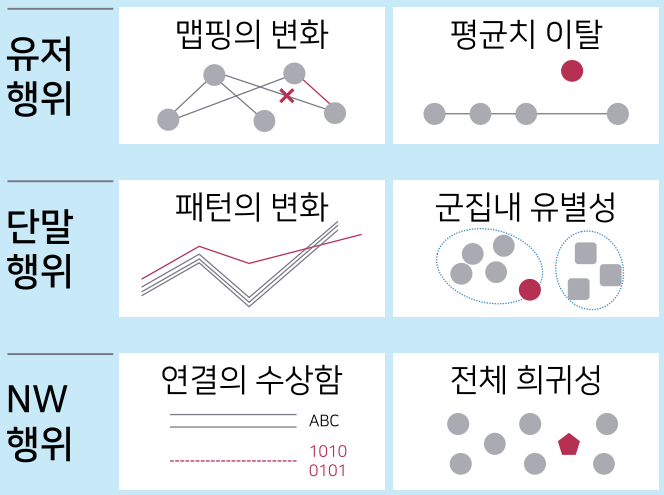
수집 및 통합

생산라인에서 발생하는
네트워크 트래픽 수집



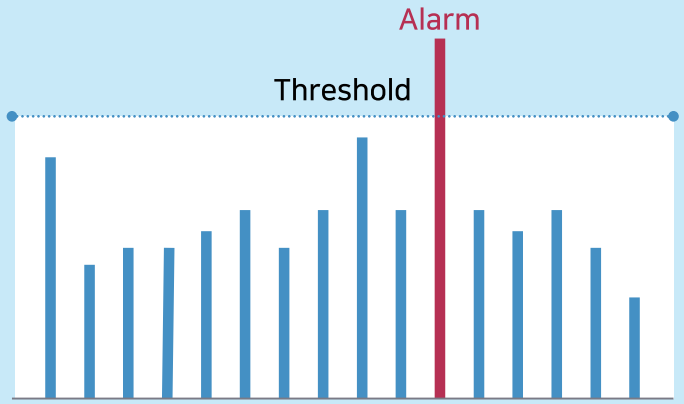
학습 및 추론

정상행위의 베이스라인 설정 및
AI기반 보안 이상징후 추론



시각화

감시, 추적, 대응을 위한
위협 시각화



네트워크 토폴로지 및
사용현황, 이상 알람 등

AI기반 위협 탐지 – Darktrace IIS

고급 이상행위 탐지기술 (Recursive Bayesian Mathematics)

- **행위 자체의 수상함**
  : Beaconing, DGA
- **군집 내에서의 유별성**
  : Clustering
- **과거 패턴과의 불일치**
  : Single Extreme Feature, Multi Extreme Feature
- **전체에서의 희귀성**
  : Rareness

Recursive Bayesian 추론 기반의
위협 확률 계산 (Classifier)

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)} = \frac{L(A|B)\,P(A)}{P(B)}$$

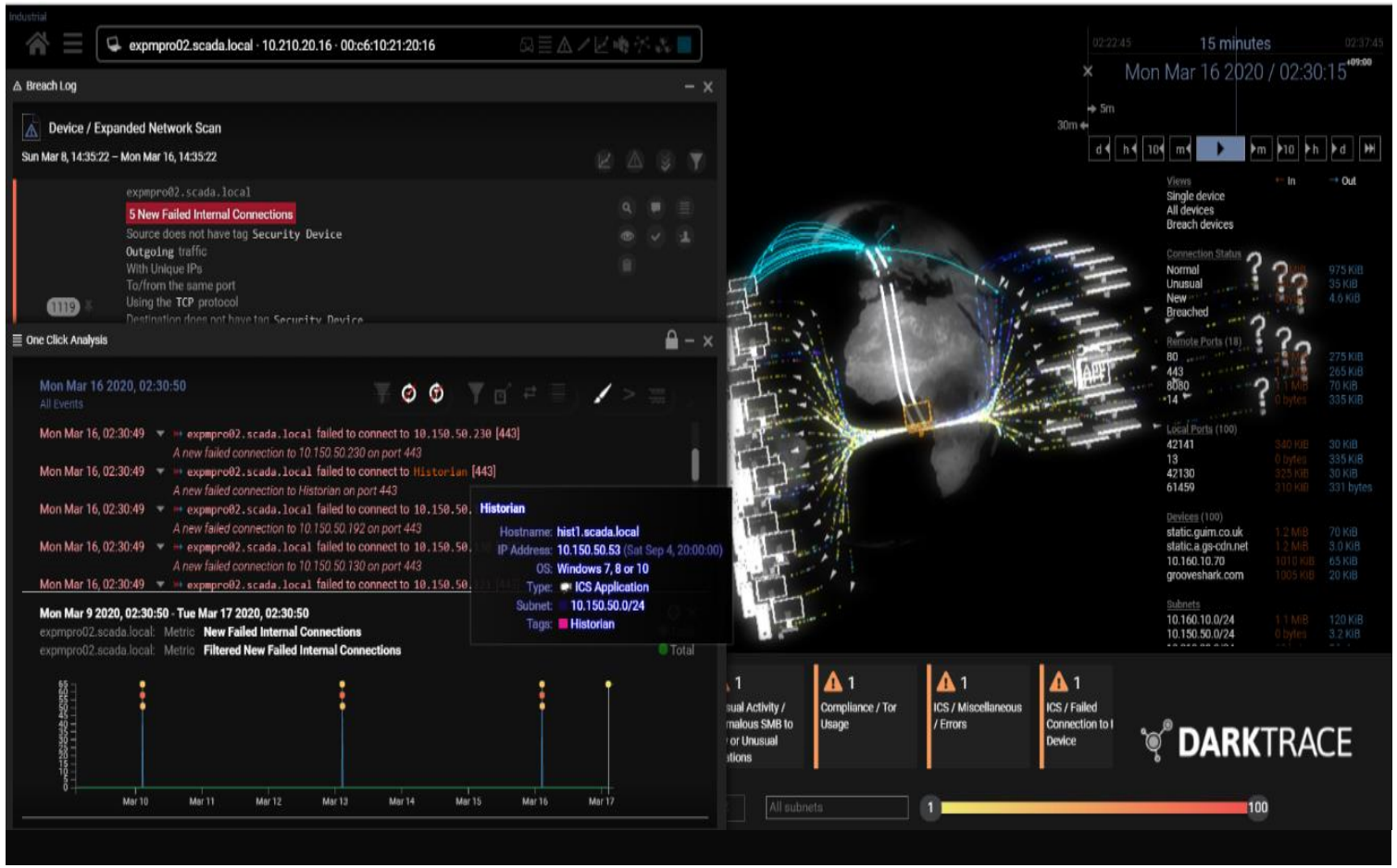
: 15%

: 60%

: 95%

AI기반 위협 탐지 – Darktrace IIS

생산라인 네트워크의 Level 1 ~ Level 4의 통신 분석을 통해 보안 이상징후 탐지 및 가시화



Traffic ▸ Visibility

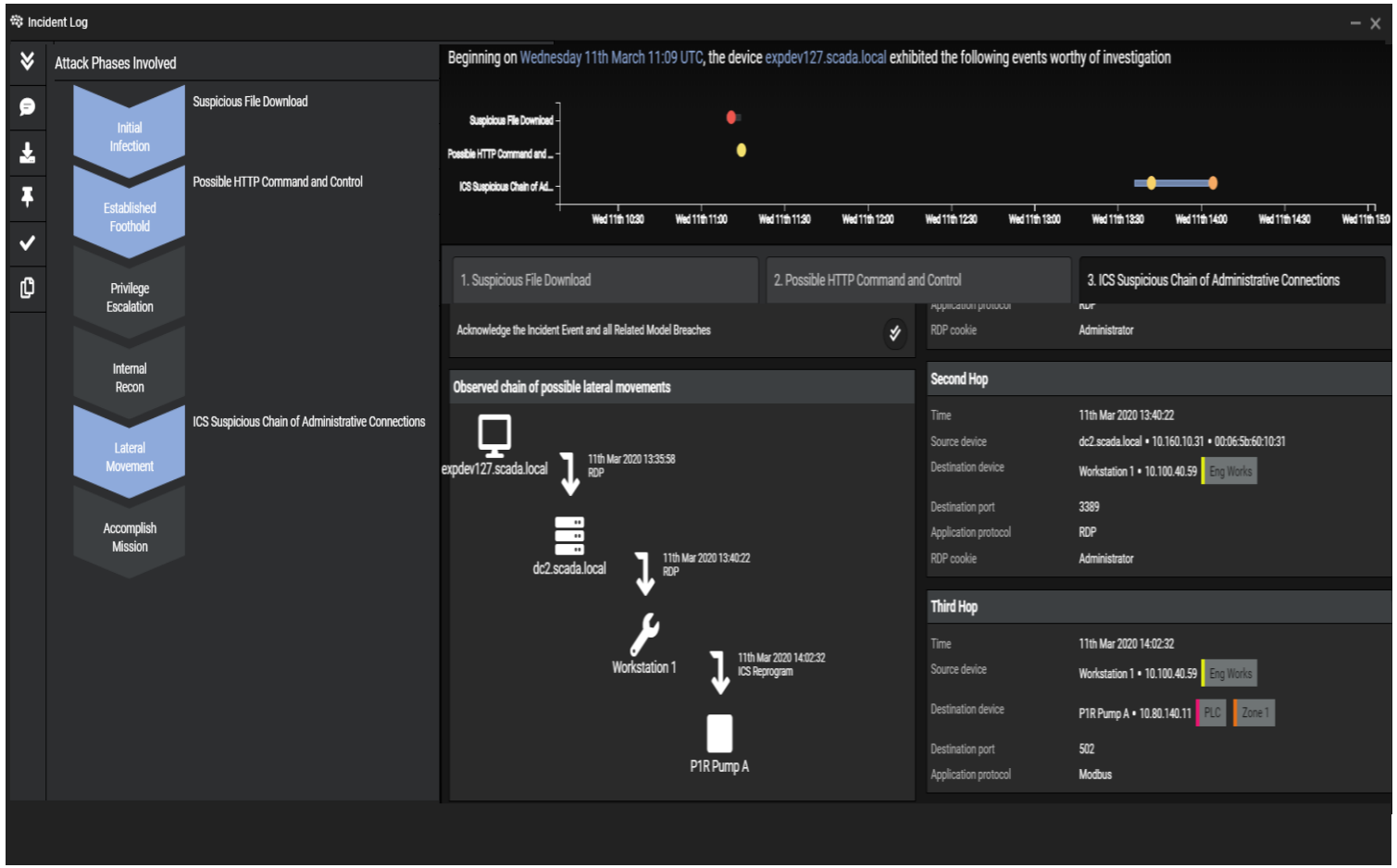
- 모든 네트워크 트래픽 정보 제공
- 어플리케이션, 호스트, 인터페이스 등의 트래픽, Session기반 정보 제공
- 특정 호스트의 트래픽 송수신 내역 확인
- 3D 위협 가시화

Event ▸ Anomaly Detection

- 평소와 다른 비정상적인 이벤트 탐지
- ML 기반 보안 이상행위 탐지 (Critical Risk Model, Baseline Model, Malicious Activity Model 등)

AI기반 위협 탐지 – Darktrace IIS

보안 이상징후(비정상/유해 트래픽, 악성코드 감염) 탐지 및 원인 분석

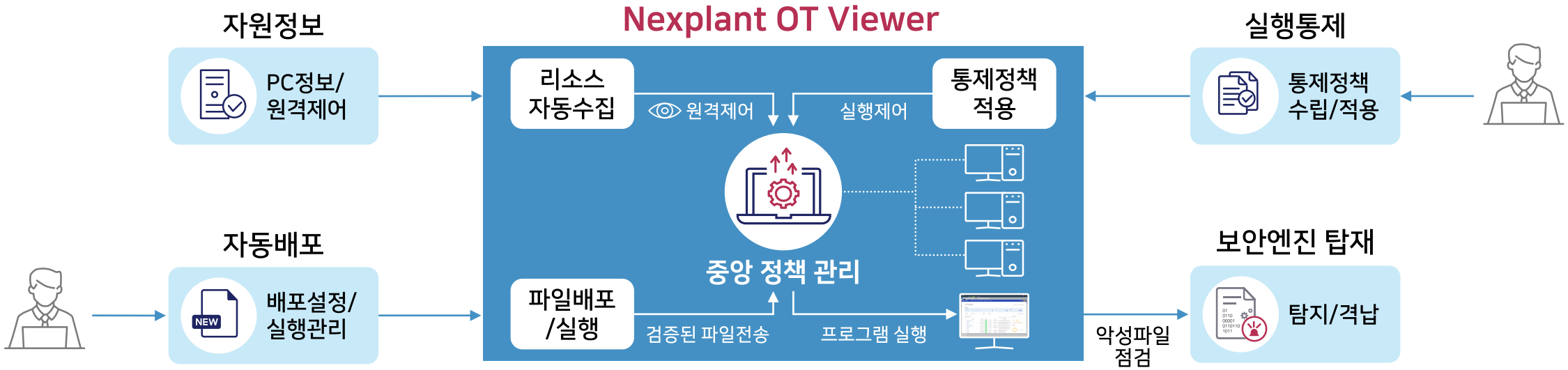


Advanced ▸ Incident Detection

- 이벤트 연결을 통한 상관분석 기능 제공
- 시나리오기반의 사이버 킬체인 제공
  (사고 원인 분석)

Endpoint보안 – Nexplant OT Viewer

자원 모니터링, 프로그램 배포/실행 관리, 보안 점검을 통하여 Endpoint 보안 통합 지원



PC 자원관리

- 제조PC 자원정보 자동 취합
- 필수 프로그램 및 정품 관리
- 원격접속(P2P)
- 원격제어(확장기능)

배포관리

- 중앙 관리의 배포 설정
- PC 성능에 따른 자동 배포
- 다양한 파일 형식 적용
- 적용/실패 이력관리

프로세스 통제

- 화이트리스트 기반 정책
- 비업무 프로그램 사용통제
- 업무그룹별 통제정책 지정
- 오프라인 정책 적용

보안관리

- 탑재된 보안엔진으로 점검
- 비정기 악성코드 점검
- 인가된 저장장치(USB) 통제
- MTP[1] 장치 통제

[1] Media Transfer Protocol : 다목적 자료전송 프로토콜(MS)

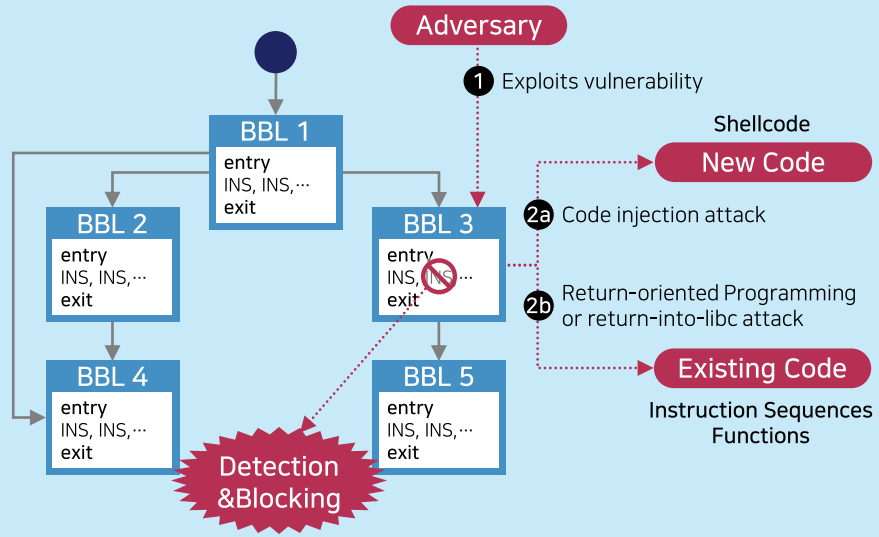
Endpoint보안 – XGuard(Karamba Security社)

설비/IoT 기기 펌웨어에 보안모듈 삽입(컴파일단계) → 어플리케이션 자체적 외부 공격(악성코드 등) 탐지/차단

CFI(제어흐름무결성)

- 프로그램이 허용된 제어 흐름대로 실행하도록 제한, 제어흐름 이탈시 실행 중단(Control-flow Integrity)

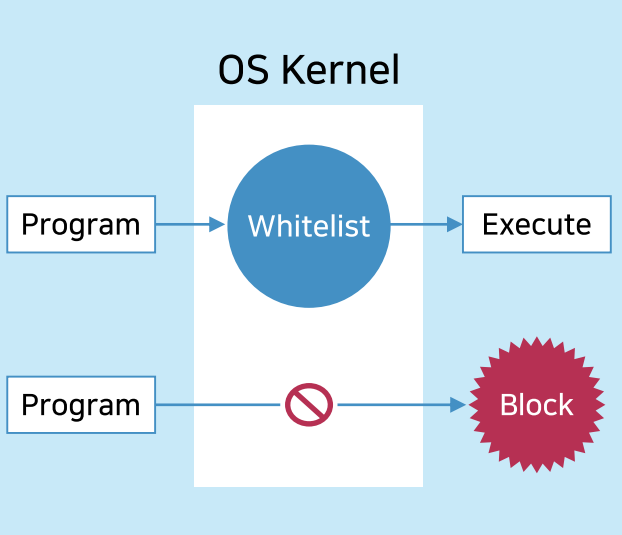
  *제어흐름 이탈 = 해킹 성공



Whitelist

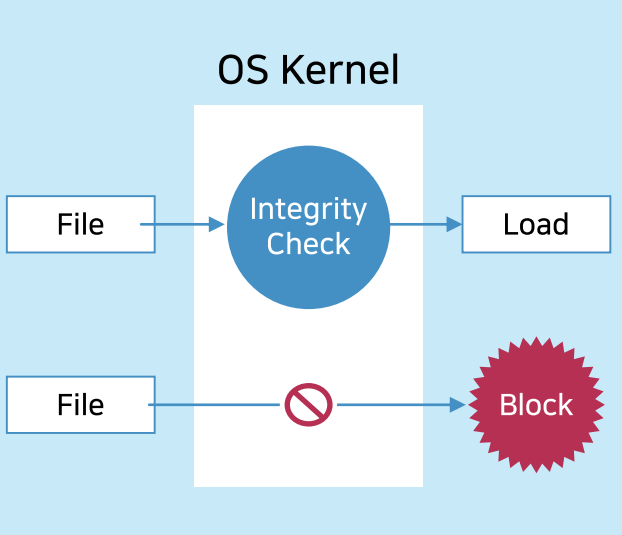
- 허용된 프로그램만 동작하도록 사전에 프로그램 리스트(Whitelist) 작성
- 장치 deploy 후 Whitelist 갱신 가능

  *Whitelist 정책에 포함되지 않은 프로그램은 실행 차단

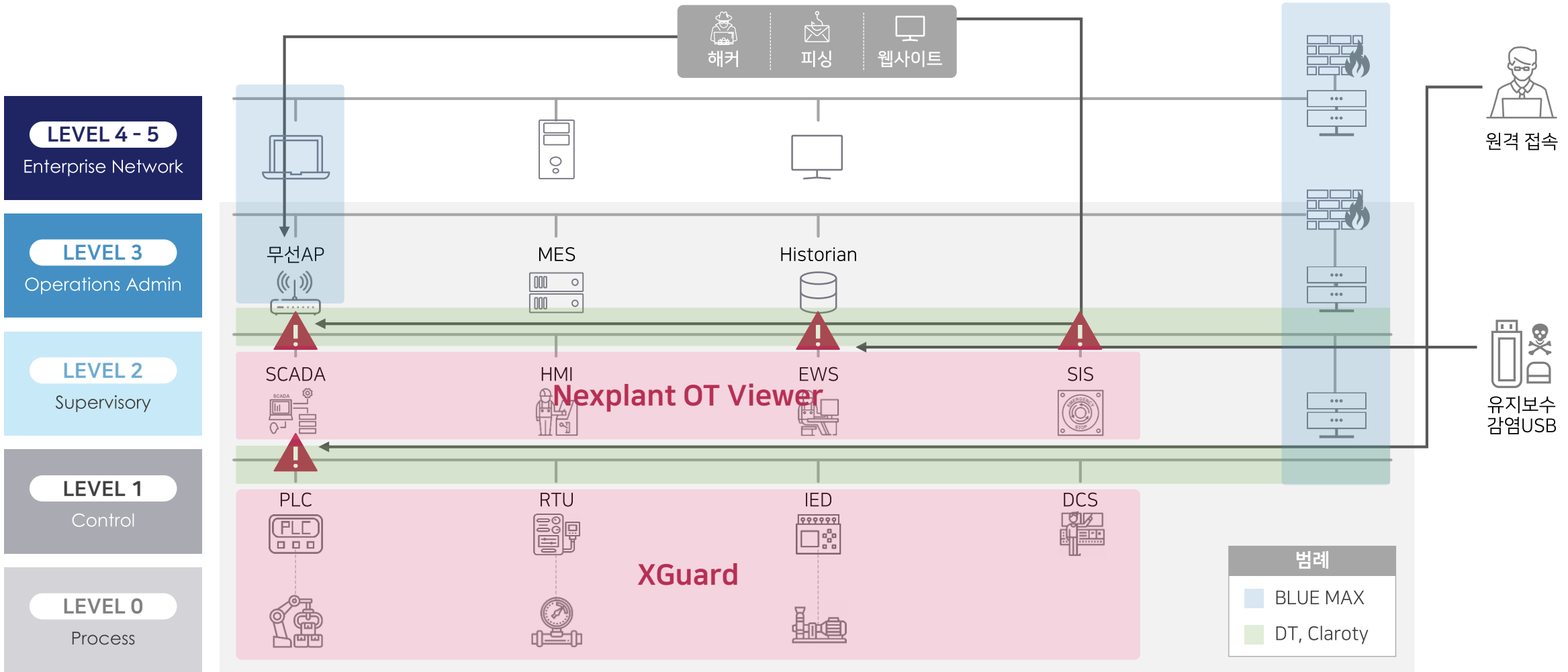


Tamper-proofing

- 지정된 파일에 대해 위·변조 차단
- 솔루션 자체 보호 및 사용자가 지정한 파일의 변조 방지

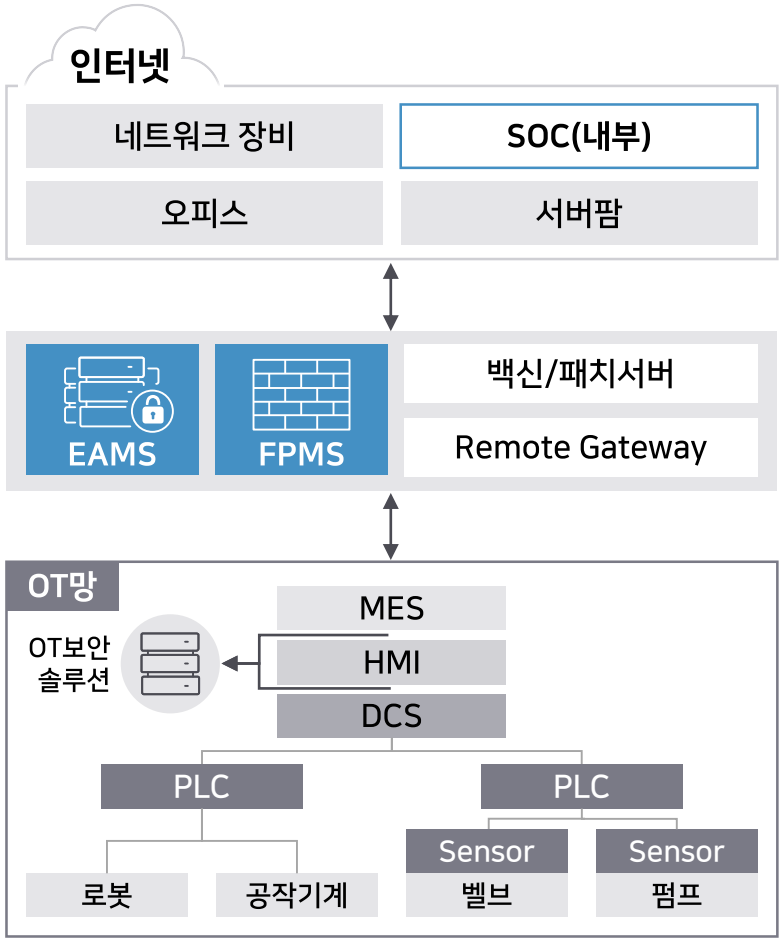


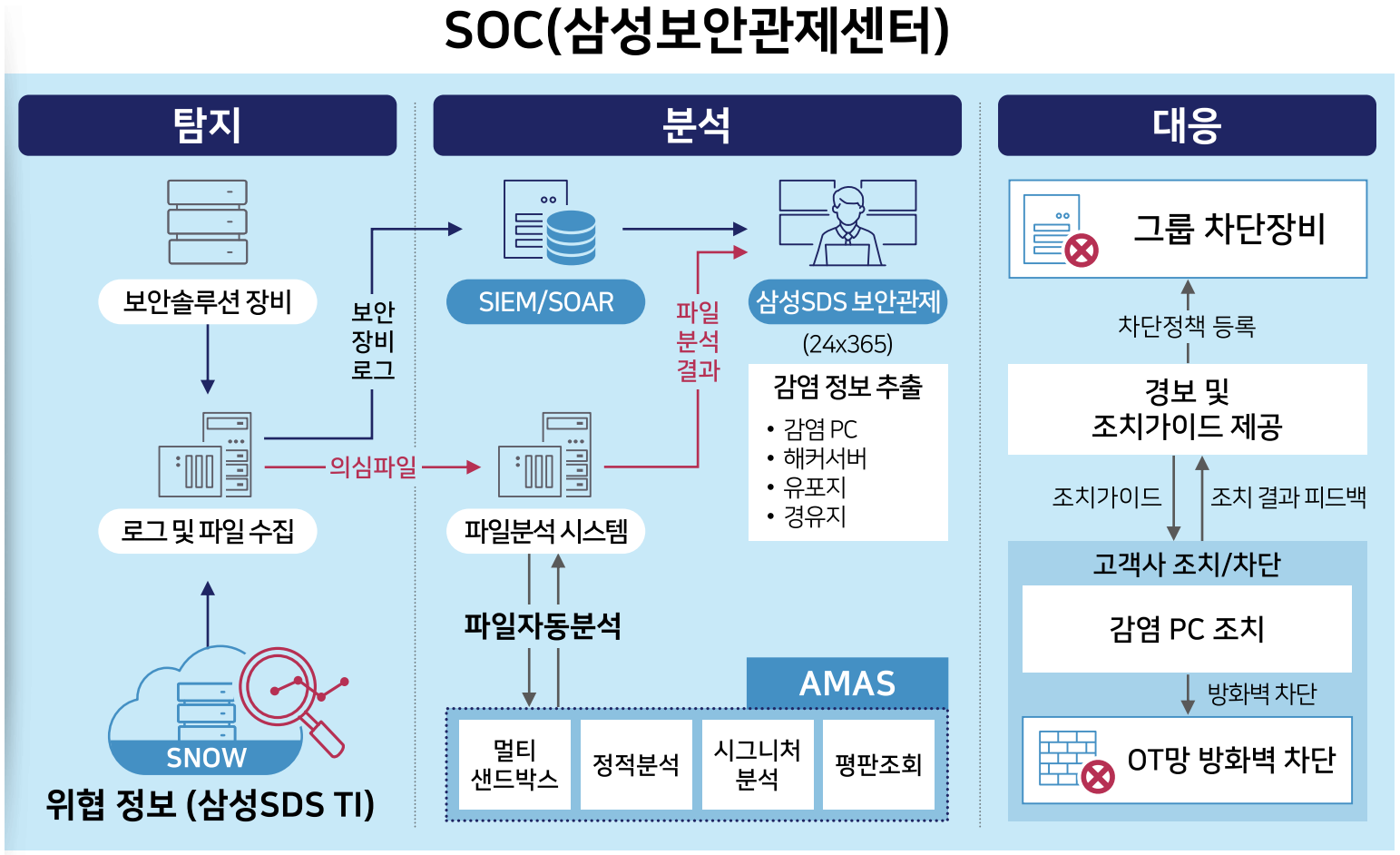
삼성SDS OT보안 Defense in Depth



삼성SDS OT보안 관제 - Architecture

Architecture상 악성코드 탐지, 이상행위 탐지를 표시





삼성SDS OT보안 관제 - 차별화 포인트

POINT 01 OT보안관제 전문성

POINT 02 24X7 Global Operation

POINT 03 보안 운영 효율화 Solution

POINT 04 다양한 관제 서비스 모델

Point 1) 보안관제 전문성/경험 보유

삼성SDS는 20년간 IT보안관제의 축적된 전문 노하우와 맨파워를 기반으로 첨단 보안관제 센터를 운영중

보안관제 Expert 조직 보유

❶ 6년이상 보안 경력보유한 인력으로 구성

❷ 삼성 관계사 대상 20년간 축적된 보안관제 노하우

❸ 전문화된 관제, CERT[1], 연구소(원천기술), 개발 조직 운영

관제 조직		CERT 조직
[1선] 1차 위협탐지	[2선] 심화 위협분석	대응 조치
개발 조직		**연구소**
솔루션 개발		원천기술 연구

[1] Computer Emergency Response Team

삼성SDS 보안관제센터 (삼성SDS 상암IT센터 5층)

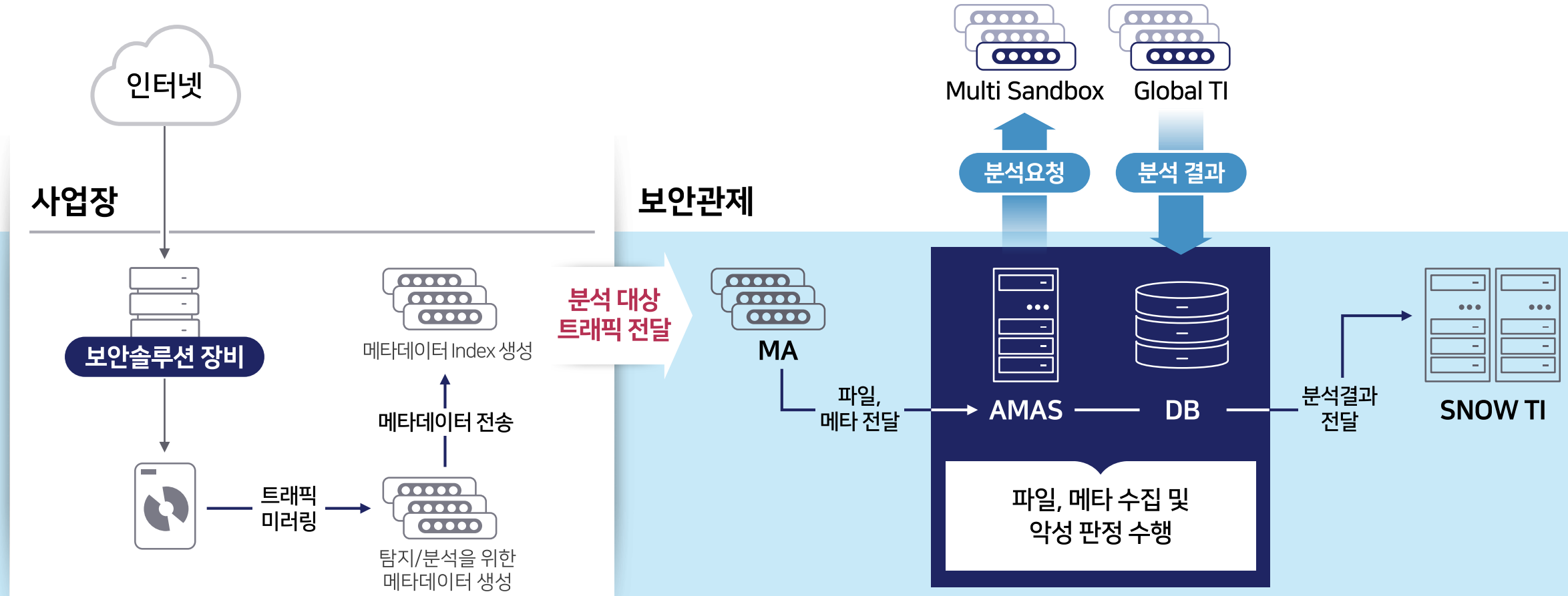
Point 2) 24X7 Global Operation

삼성SDS는 현재 Global 63개국,27개 계열사 대상으로 500,000 장비 모니터링, 17TB이상/日 보안 이벤트수집
3,000개/日 의심파일 분석, 160개/日 위협정보 관리하는 운영 역량 보유

* 한국/미주 보안관제센터에 주・야간 24시간 근무체계 가동

Point 3) 보안운영 효율화 솔루션 – AMAS[1]

트래픽 수집 → 파일, 메타 추출 → 분석 → 악성판정 → 결과 전달하는 악성코드 자동분석 시스템



[1] Auto Malicious Analysis System: 삼성SDS에서 자체 개발한 악성코드 분석 시스템

Point 3) 보안운영 효율화 솔루션 - SNOW TI[1]

각 관제에서 수집되는 정보 및 글로벌 최신 보안위협 정보를 실시간으로 수집 – 분석 및 가공하여 대내외 보안관제 정책에 활용

삼성 보안관제센터

SIEM | APT포렌직 | 웹메일

악성코드 | IPS | Anti-DDoS | 방화벽

사고조사 분석결과 | 해커서버 추출기

*기 수집정보 및 중복 건 제외 ('20.12월 기준)

글로벌 외부 위협정보

3rd Party | 금융보안원

OSINT[2] | KISA | 보안 리포트

보안 뉴스레터 | 보안 블로그 | 해커 SNS

일 2.7만+ 누적 1천만+

악성사이트 정보
공격자IP, C&C, 경유지/유포지

일 0.8만+ 누적 3백만+

악성파일 정보
악성코드 해시, 태그 정보

일 400+ 누적 17만+

악성메일 정보
발신자 메일주소, 메일제목

[1] SNOW TI: Samsung kNOWledge Threat Intelligence
[2] OSINT : Open Source Intelligence

Point 4) 다양한 관제 서비스 모델

· **파견관제** : 보안관제 모니터링을 현장에서 수행하며, 높은 이해도를 바탕으로 원활한 보안관제 가능
· **하이브리드관제** : 현장 및 원격관제로 이원화하여 보안이슈 발생 시 사업장/삼성SDS 협업대응 가능
· **원격관제** : 가장 저렴한 비용으로 24x365 보안관제 서비스 제공

관제 운영 방안	파견관제	하이브리드관제	원격 관제
투입인력	전체인력 파견	파견 및 원격관제	전체인력 원격
근무지	주·야간 : 사업장(Dedicated)	주간 : 사업장(Dedicated) 야간·주말 : 삼성SDS(원격, 관제 Shared)	주·야간 : 삼성SDS (원격, 관제 Shared)
장 점	• 관제인력 전담 배치로 업무 집중도 증대 • 현장 이해도가 높아 보안업무 밀착지원 • 야간 긴급이슈 발생 시 현장대응 가능 • 신규 위협분석 및 탐지정책의 상시관리 • 보안시스템 정책운영 및 가용성 모니터링	• 이슈발생 시 원격 관제센터와 협업대응 • 파견 및 원격관제 혼용으로 인력관리 수월	• 비용이 가장 저렴 • Shared 관제로 외부이슈에 민첩대응 가능

OT보안 발전 방향

현재 정보보호 중심의 위협 대응에서 향후 무중단 생산의 중심으로 OT보안 발전

위협 대응 중심

- 각 영역/Level별 위협 대응 솔루션 적용
- OT전용 솔루션 출시

On-Premise

+ AI

- 보안 사고 시 복구 강화
- 솔루션 통합 및 AI 본격 적용

Cloud/Service

무중단 생산으로 확대

- 중단 없는 생산을 위해 정보/물리보안, 장애 방지, 예지보전, 환경/오염/안전 통합 관제 및 Recovery를 포함한 대응

CIAS — Confidentiality, Integrity Availability, Safety

Sustainability — 사회/환경 친화 생산

Thank you

SAMSUNG SDS