GAMES ON AWS 2026

aws FOR GAMES

AI 에이전트 시대의 게임 클라우드 보안

모델 밖의 책임과 공격 경로

GS 네오텍 | 박제호

GS Neotek | MEGAZONE CLOUD

회사 및 부스 소개

GS 네오텍 소개


GS Neotek
AI
• 도메인별 FDE 컨설팅 지원
• 산업별 특화된 AI Agent 구축
• AX 전문 플랫폼 MISO 지원
Cloud
• 멀티 클라우드 설계·구축·운영
• 전문 매니지드 서비스 제공
• FinOps 비용 최적화·24/7 모니터링
Security
• 실행 가능한 컴플라이언스 보안 컨설팅
• CNAPP 솔루션 기반 위협 통합 관리
• AI 레드티밍·보안관제로 지속 개선 환경 구현
GS네오텍은
AI로 혁신하고
클라우드로 확장하고
보안으로 지킵니다

Build with AI, 그 시작을 GS네오텍과 함께

만들고 · GPU 인프라 → 사용하고 · LLM 활용 → 지킵니다 · 클라우드 보안







1 Compute Lens

Enterprise GPU as a Service

고성능 GPU 자원을 작업별로 나누고 하나의 콘솔에서 운영하는 GPU as a Service 솔루션

- **작업 맞춤형 GPU 분할**
  에셋 생성·NPC AI·추론까지 소프트형/격리형 선택
- **사용 시간 기반 과금·용량 예약**
  쓴 만큼 과금, 수요가 몰리는 기간엔 용량 예약
- **분산 GPU 통합 운영**
  스튜디오·프로젝트별 GPU를 한 곳에서 운영

2 ETAGIA

LLM GATEWAY

팀마다 쓰는 LLM을 한곳에 모아 보안·비용까지 통제하는 기업용 AI 게이트웨이

- **지능형 LLM 라우팅**
  작업별 모델 자동 선택, 장애 시 다음 모델로 전환
- **민감 정보 유출 차단**
  기획서·API 키·개인정보를 외부 전송 전 차단
- **실시간 AI 비용 관리**
  프로젝트별 실시간 정산, 예산 초과 사전 알림

3 Security Lens

자산부터 컴플라이언스까지 통합 관리하는 AI 기반 CNAPP+ 솔루션

- **통합 보안 가시성**
  클라우드부터 게임 서버·빌드 코드까지 한 흐름으로
- **AI 기반 보안 운영**
  AI가 오탐을 정제하고 조치 우선순위 제시
- **컴플라이언스 내재화**
  ISMS-P 대응 증적을 운영 데이터로 연결

이번 세션을 통해 확인할 내용

01 식별

AI와 함께 운영되는 자산은 무엇이며
어떤 법적 의무를 확인해야 하는가

02 연결·영향

자산·권한·데이터는 어떻게 연결되고
게임 서비스에 어떤 영향을 주는가

03 결정

무엇을 먼저 줄이고
조치 결과를 어떻게 확인할 것인가

컴플라이언스 관점의 보안

보안 이슈가 발생한다면, 기술 조치만으로 끝날까요?

가상 시나리오 | 공격자가 챗봇에 악성 프롬프트를 넣어 타 이용자의 개인정보를 취득했다고 가정한다면, 공격 경로를 찾아 막으면 끝일까요?

01 공격자의 악성 프롬프트 입력 → 02 AI 챗봇 전달 → 03 백엔드 도구·API 수행 → 04 워크로드 IAM 역할 수임 → 05 이용자 개인정보 접근

보안 이슈가 발생한다면, 기술 조치만으로 끝날까요?

가상 시나리오 | 공격자가 챗봇에 악성 프롬프트를 넣어 타 이용자의 개인정보를 취득했다고 가정한다면,
공격 경로를 찾아 막으면 끝일까요?

01 공격자의 악성 프롬프트 입력 → 02 AI 챗봇 전달 → 03 백엔드 도구·API 수행 → 04 워크로드 IAM 역할 수임 → 05 이용자 개인정보 접근

**적용 법규·통지 요건, 영향 범위, 조치 후 검증과 증적은
누가 판단하고 대응하고 있습니까?**

게임 보안 사고는 계정·공급망·운영·데이터 전반에서 발생합니다

계정·운영 권한	R사 플랫폼 인기 게임 개발자 계정 탈취 신고(2025) 게임 소유권 이전·인게임 결제 악용 주장
소프트웨어 공급망	국내 게임 보안 모듈 변조(2024) 공식 게임 설치 경로로 악성코드 배포
라이브 운영 설정	M 온라인 게임 운영 권한 사고(2025) 전 계정에 GM 권한 부여, 서버 중단·롤백
서버·개인정보	F사 서버 침해(2024) 직원·협력사 개인정보 2,606건 유출

AI 보안 도구의 확산과 사례 발생

오픈소스 AI 보안 검증·자율 침투 도구 예시

ARTEX
CyberStrike AI
PentAGI
Strix
Shannon
PentestGPT

도구를 활용한 침투 사례

실제 사례 100자 미만 중국어 지시로 AI 에이전트가 수시간 자율 탐색·침투
1,200곳 이상 시도, 100곳 이상 침입 성공 보도, 성공 프로젝트 평균 23시간
DeepSeek·Claude Code 조합 추정, 토큰 약 5천 달러·성공 1건당 약 50달러 추산

출처: Reuters/연합뉴스(2026.10), NorForge · 침입·비용 수치는 보도와 연구자 추정

치명적 CVE와 NVD 대응 부담 증가

CVE	대상 제품	CVSS	취약점과 잠재 영향
CVE-2026-109618	PHP Core	9.2 v4	OOM 처리 결함으로 비인증 원격 코드 실행 가능
CVE-2026-109619	PHP Core	9.2 v4	요청 간 전역 상태 재사용으로 원격 코드 실행 가능
CVE-2026-110264	GitLab CE/EE	10.0 v3	정규식 컴파일러 정수 오버플로, 조건부 비인증 RCE
CVE-2026-114625	VeloCloud Orchestrator	9.9 v3	인증된 사용자 SQL 삽입, 운영자 권한 획득
CVE-2026-104286	FortiMail	9.8 v3	비인증 경로 순회, 임의 파일 쓰기 가능

출처: 각 제품 보안 공지·CVE CNA · NIST NVD 운영 발표(2026.4)

- CVE: Common Vulnerabilities and Exposures (공통 취약점 및 노출)
- NVD: National Vulnerability Database (미국 국가 취약점 데이터베이스)

사이버 복원력법(CRA)가 요구하는 취약점·보안사고 보고

EU 사이버복원력법(CRA) 제14조

신고 유형	판단 기준	최종 보고
실제 악용된 취약점	허가 없는 실제 악용의 신뢰할 증거가 있는 제품 취약점	시정·완화 조치 제공 후 14일 이내
중대한 보안사고	제품의 가용성·진정성·무결성·기밀성에 심각한 영향	72시간 본 통지 후 1개월 이내

인지 시점 기록 → (1차) 24시간 조기 통지 · (2차) 72시간 본 통지 · (3차) 사고 처리 후 1개월 이내 ENISA 단일 신고 플랫폼 보고

PC 다운로드형 클라이언트 게임이나 모바일 앱 형태의 비디오 게임 역시 CRA가 규정하는 '디지털 요소가 포함된 제품'에 포함

2026.9.11 취약점·중대 사고 보고 의무 적용
2027.12.11 제품 보안 일반 의무 전면 적용

출처: EU Regulation 2024/2847 제14·71조 · 적용 제품 여부는 별도 검토

- CRA : Cyber Resilience Act (사이버 복원력법)

SBOM(Software Bill of Materials, 소프트웨어 자재 명세서) 요구

지역별 SBOM 요구 수준

관할	주요 적용 대상	요구 수준·시점
EU CRA	적용 디지털 제품 제조자	2027.12.11부터 SBOM 작성·기술문서 연계, 적합성 절차
미국 연방 조달	기관 조달 소프트웨어	OMB 위험기반 지침: 계약에 따라 최신 SBOM 요청 가능
미국 FDA 524B	해당 사이버 의료기기	2023.3.29부터 시판 전 신청에 SBOM 제출 의무
한국 공공	공공 IT 시스템·제품	2027년 제출 제도 도입 발표, 세부 요건 확인 필요

CISA 2026 최소요소: 17개 데이터 필드 권고 · EU CRA는 SBOM 일괄 공개 의무 아님
일반적으로 SPDX·CycloneDX로 구성요소 관리

출처: EU CRA · OMB M-26-05 · FDA 524B · 과기정통부 공공 SW 공급망 정책

AI-BOM 권고안

영역	기록할 내용	게임사 AI-BOM 속성 예시
메타데이터	소유 조직·작성자·버전·갱신일	상담봇 책임팀, 릴리스 2.3, 변경일
시스템	목적·구성·의존성·입출력 흐름	게임 클라이언트→상담 API→모델→DB
모델	모델 ID·공급자·출처·사용 제약	외부 LLM 버전, 파인튜닝 여부, 사용 제한
데이터셋	학습·검색 데이터 출처·권리·민감도	FAQ, 플레이어 문의, 개인정보 등급
인프라	실행 계정·배포 위치·하드웨어	AWS 계정, Amazon Bedrock, GPU 환경
보안	접근통제·가드레일·취약점·평가	IAM 역할, 도구 허용목록, 침투 평가
KPI	성능·안전 지표·측정법·갱신 주기	오답률, 민감정보 노출률, 월간 평가

CISA·G7의 비의무 권고이며 CRA의 SBOM 작성 의무와 별개

출처: CISA·G7, Software Bill of Materials for AI – Minimum Elements

인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 (AI 기본법)

인공지능기본법 진행 경과

2024.12	국회 본회의 통과
2025.01	공포
2026.01.22	최초 시행
2026.07.21.	개정법 시행

사실조사·시정·과태료

제40조 - 위반 의심·신고 시 자료요구·현장조사
조사 후 위반행위 중지·시정 명령 가능

제43조 - 사전고지 누락·국내대리인 미지정·명령 불이행에 3천만원 이하

정부 - 2026.1.22부터 최소 1년 계도 방침
(종료일 별도 확인 필요)

AI 도구 제공자와 게임 콘텐츠 제작자의 법적 역할

인공지능사업자: 인공지능기본법상 의무 주체

인공지능개발사업자

외부 AI 제공자

모델·AI 시스템을 개발해
게임사에 제공 (특수/범용)

AI 제공 →

인공지능이용사업자

AI 제품 및 서비스 제공사

외부/내부 AI 기반 제작 도구 운영
제작사에 AI 제품·서비스 제공

제품·서비스 제공 →

개별 법령 소관 영역

이용자

게임 콘텐츠 제작사

AI로 원화·영상을 만든 뒤
게임 콘텐츠에 활용

게임 콘텐츠도 AI 결과물 활용만으로 AI 제품·서비스가 되는것은 아님. 이용자와 인공지능 사업자의 구분이 필요

출처: 인공지능기본법 제2조· 인공지능기본법 시행 관련 추가 설명

게임사는 AI 기능별로 적용 지위를 판단

게임사가 이용자인 경우

외부 AI로 원화·시나리오 초안 작성
사람이 편집해 고정 콘텐츠 배포
플레이어에게 AI 기능은 제공하지 않음

게임사가 인공지능이용사업자인 경우

외부 AI를 게임 기능에 연결
플레이어가 대화·생성 기능을 사용
게임사가 AI 서비스를 운영·제공

게임사의 인공지능기본법 투명성 의무

적용 판단	인공지능사업자 지위와 생성형·고영향 여부를 기능별로 확인
사전 고지 (31①)	생성형·고영향 AI 기반 운영 사실을 이용 전 약관·로그인 화면 등에 고지
생성물 표시 (31②)	생성형 AI 결과물에는 생성 사실 표시, 이용 화면과 반출 파일의 표시 방식을 구분
실사형 결과 (31③)	실제와 구분 어려운 음향·이미지·영상은 명확하게 표시, 창작물 예외 방식 검토

출처: 인공지능기본법 · 인공지능기본법 시행 관련 추가 설명

담당자가 확인해야 할 포인트

무료·비영리	AI 제품·서비스를 제공한다면 무료·비영리여도 사업자 의무 검토
기존 서비스	시행 전 출시했어도 시행 후 생성물은 표시, 과거 제공물 소급 표시는 불필요
챗봇 표시	대화 화면에 인식 가능한 로고 등 표시, 답변마다 워터마크 불필요, 단 합리적 수준
표시 방식	일반 생성물: 비가시적 표시 가능 (메타데이터, 워터마크 등) 인공지능 조작 영상(딥페이크): 가시적 표시만 허용, 창작물 예외 검토 가능

인공지능 기본법에 따라 게임 영상(예술적·창의적 표현물) 등에도 창작물 예외를 검토 가능. 크레딧·메타데이터·설명 다양한 방법으로 표시 가능

출처: 인공지능기본법 · 인공지능기본법 시행 관련 추가 설명

AI 거버넌스 기준과 클라우드 보안 지침

일반적으로 활용되는 AI 관리 프레임워크

NIST AI RMF 1.0

Govern · Map · Measure · Manage
AI 위험을 수명주기 전반에서 관리하는 자발적 기준

ISO/IEC 42001:2023

AI 경영시스템(AIMS)의 요구사항
조직의 정책·책임·평가·개선을 심사·인증 가능

클라우드 AI 거버넌스 프레임워크 사례

AWS AI Security Framework

인프라, 신원·데이터, AI 앱의 3계층 통제
예: IAM·AgentCore Identity·Amazon Bedrock Guardrails

Microsoft Zero Trust for AI

명시적 검증·최소 권한·침해 가정
예: Microsoft Entra Agent ID

Google Secure AI Framework (SAIF)

AI 시스템·공급망 위험을 평가하고 통제
예: SAIF Risk Self Assessment

중국의 범국가적 AI 에이전트 신원 구현 시작

사내 프로세스 ID를 넘어, 국가가 통제권을 쥐겠다는 규제 프레임워크

상호운용	GB/Z 185–2026: 에이전트 신원 코드와 자격의 상호 인증 (크로스 플랫폼)
책임 추적	등록 서비스·개발·운영 주체와 에이전트 활동의 연결 (하드웨어/블록체인/실명 연결)
지역 시범	베이징 Yuri: 가상 아티스트 신원 인증과 활동 관리
권한 검증	국가 규정(3등급 권한 모델) 기반 법적 인가 정책 검증

AI 에이전트, 휴머노이드 로봇 등 다양한 영역에서 전체 통제를 목적으로 함

AI 인프라, 데이터, 권한 등 연관된 자산을 어디까지 식별하고 있는가

자산 분류 기준

분류		설명	예
전자정보		- 전자적 형태로 저장되는 데이터	- 데이터베이스, 데이터파일 등의 전자파일
문서		- 종이 매체로 된 정보자산 - 업무에 사용/산출되는 문서나 기록물	- 규정 및 지침, 각종 대장, 계약서 및 협약서 등
소프트웨어 자산		- 상용 또는 자체 개발된 소프트웨어나 하드카피로 보관 중인 각종 소프트웨어 자산	- 애플리케이션 소프트웨어, 시스템 소프트웨어, 개발도구 및 유틸리티
하드웨어 자산	서버	- 대내외 서비스 및 업무를 위해 사용되는 서버 자산	- 유닉스 서버, 윈도우 서버 등
	개인용 컴퓨터	- 임직원이 사용하는 개인 컴퓨터	- PC, 노트북, 이동형 단말기 등
	네트워크 장비	- 네트워크와 관련된 장비	- 라우터, 스위치, 허브 등
시설		- 시스템 설치, 운영 장소 - 물리적 공간 및 각종 부대시설	- 전산실, 사무실, 방재실, 통신 장비실 등
지원설비		- 전력공급, 환기시설, 방재 시설 등 정보 시스템 운영을 지원하기 위한 설비	- 항온·항습기, UPS, 공조장비 등
인력		- 소유자, 사용자, 운영자, 개발자 등 시스템 운영 및 업무 수행 중인 모든 인력	- 내부직원, 협력업체 등



?



AI 인프라, 데이터, 권한 등 연관된 자산을 어디까지 식별하고 있는가

서버 목록

자산분류	서버
설명	사용자에게 특정 서비스를 제공하기 위한 기능의 운영체제 및 프로그램이 설치되어 있는 장비

No	자산정보							
	구분	자산코드(있을 시 기입)	자산명	설명	운영체제	기종	대수	위치
ex)	윈도우 서버	ABC-000	WEB_server	웹 서버	window server	HP	1	IDC

정보보호시스템 목록

자산분류	정보보호시스템
설명	서비스 보안 운영을 위한 장비

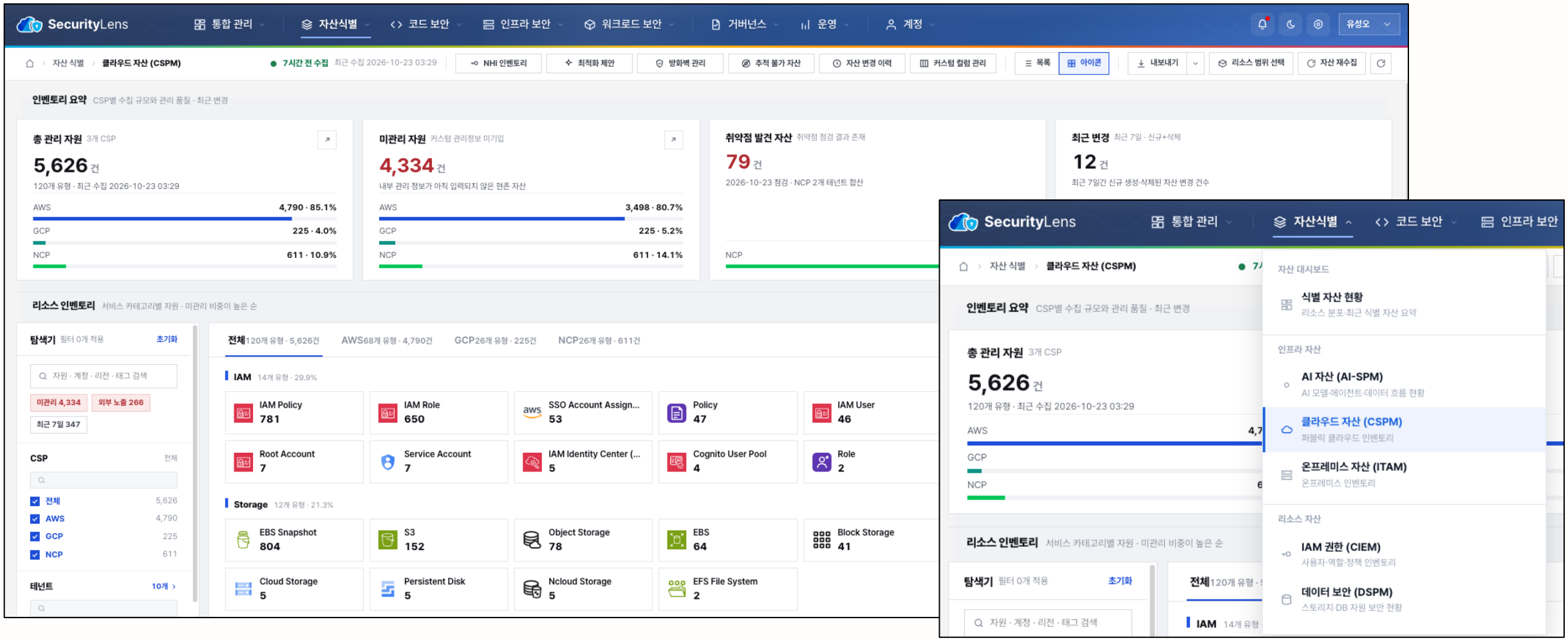
No	자산정보							
	구분	자산코드(있을 시 기입)	자산명	설명	운영체제	기종	대수	위치
ex)	UTM	0000-0000	방화벽(UTM)	외부/내부 보안	전용 OS	OOOO 0000	1	본사

DBMS 목록

자산분류	DBMS
설명	사용자가 데이터에 접근하여 데이터를 저장 및 관리 등의 기능을 제공하는 응용 소프트웨어

No	자산정보								
	구분	자산코드(있을 시 기입)	자산명	버전	유형(DBMS)	용도	대수	설치 플랫폼(OS)	위치
ex)	DBMS	SYOPT-01	DB_01	XX.XXX.XX	MS-SQL	고객DB	1	Windows 2008 R2	본사

Security Lens를 통한 CMDB를 운용하여 자산을 효율적으로 관리



자산의 연결과 영향 범위를 어떻게 볼 것인가

01 공격자의 악성 프롬프트 입력 → 02 AI 챗봇 전달 → 03 백엔드 도구·API 수행 → 04 워크로드 IAM 역할 수임 → 05 이용자 개인정보 접근

목록만으로는 복잡하거나 관리되지 않은 환경일수록 “어디까지 연결되는가”를 정확하게 답하기 어려움
Security **Ontology**를 통해 근거 기반의 의미적 답안을 만들어낼 수 있도록 접근

자산의 연결과 영향 범위를 어떻게 볼 것인가

온톨로지(Ontology)란

온톨로지(Ontology)는 특정 도메인의 지식을 컴퓨터가 이해하고 처리할 수 있도록
개념(Entity), 속성(Attribute), 관계(Relationship), 규칙(Rule)을 체계적으로 구조화한 '지식의 지도(설계도)'



온톨로지 솔루션 사례

AWS – COA (Context Ontology Accelerator)
Databricks – Genie
GSN – ODC (Ontology Development Copilot)

Security Ontology 구성하여 관계성 확보



주요 판단 포인트

- **자산**
클라우드 인프라 등 CSPM 정보 등

- **취약점**
취약점 정보 및 CVE 정보 등

- **위협**
내/외부자 공격/장애 시나리오

- **위험**
위험 시나리오

- **운영**
현실세계 조직도 반영

무엇부터 해결해야 하는가

A 점수만 본다면

CVSS/컴플라이언스 상위 취약점부터 일괄 대응

낮은 점수의 진입점과 과도한 권한의 조합을 놓칠 수 있음

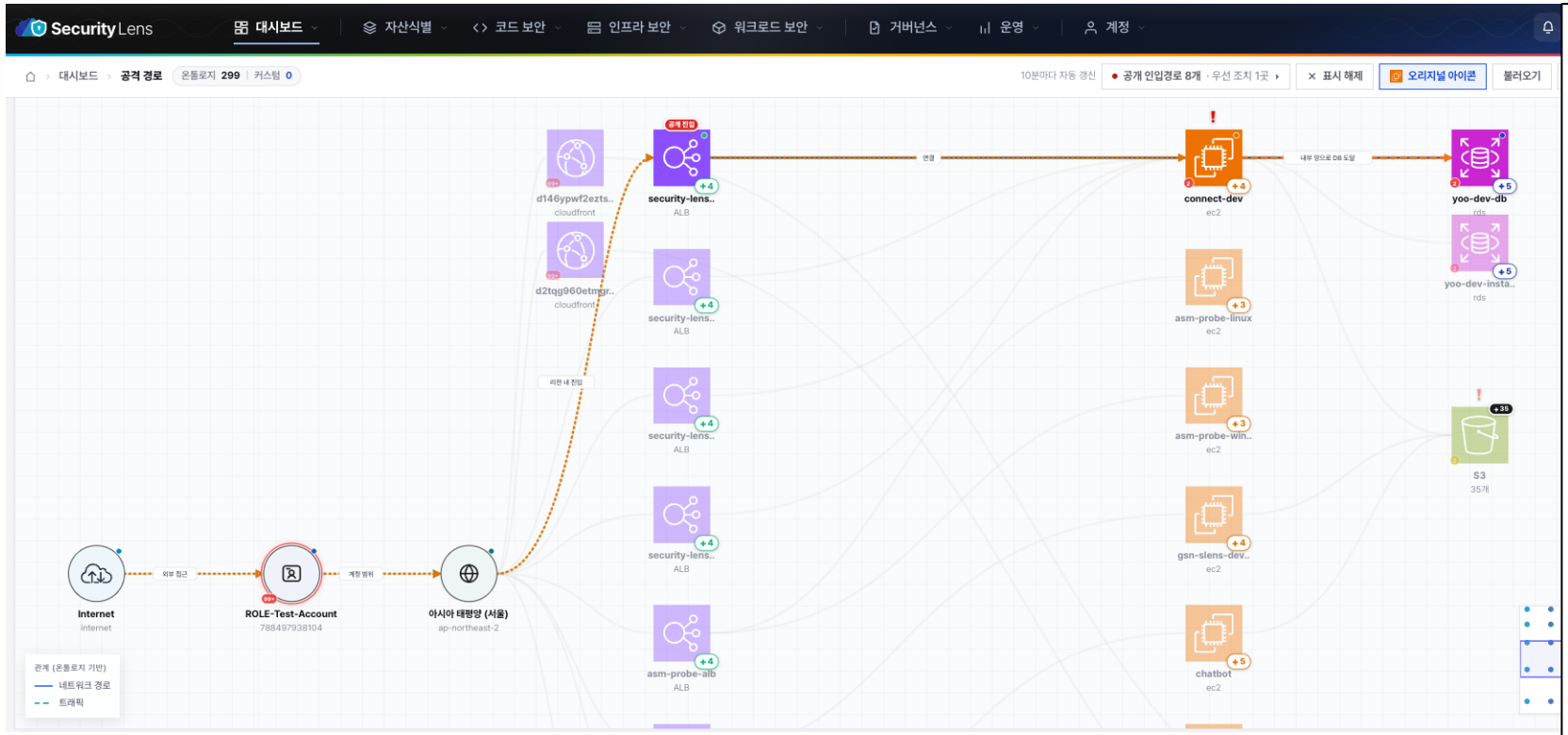
B 연결을 본다면

진입 가능성 → 실행 권한 → 중요 데이터·운영 영향

악용 시그널들과 영향 범위, 지표를 함께 평가해 먼저 대응할 위험 결정

Security Lens의 공격 경로 화면에서 실제 접근 가능여부 확인

연결된 자산에서 실행 조건을 검증하고 우선 대응 경로를 식별



주요 판단 포인트

- 진입 조건
누가 접근 가능한가

- 권한 조건
허용되는 행위

- 업무 영향도
연결된 범위 정도

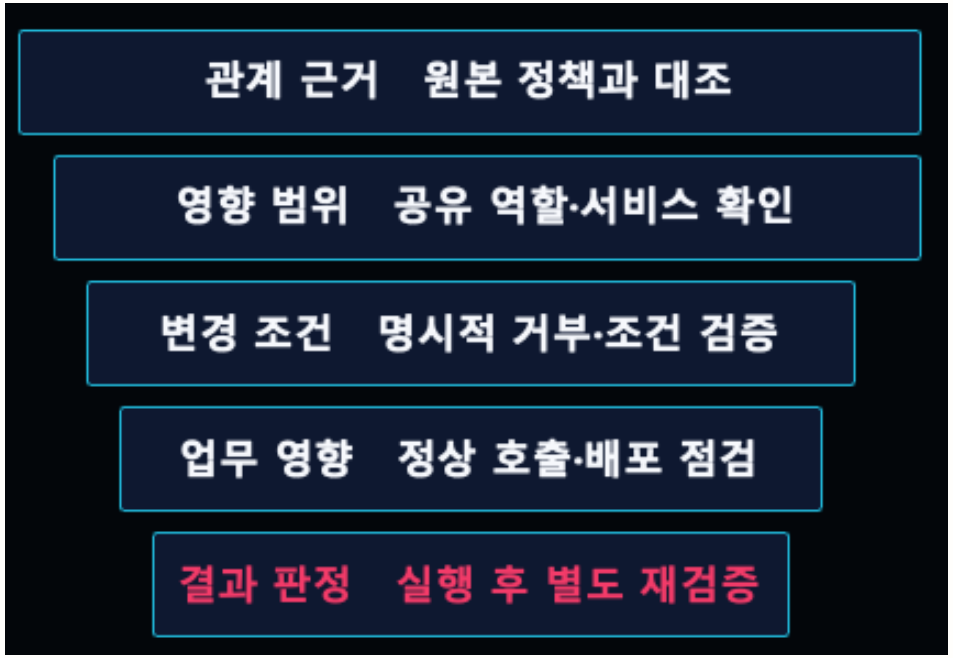
- 근거와 시점
자산의 상태와 연결되는 조합

- 우선순위
가장 위험하다고 판단한 경로 도출

Security Lens의 공격 경로 화면에서 실제 접근 가능여부 확인

연결된 자산에서 실행 조건을 검증하고 우선 대응 경로를 식별





화면의 차단 예상 효과와 실행 후 검증 결과를 구분

보안 에이전트를 방어자도 적극 활용이 필요

AWS Security Agent

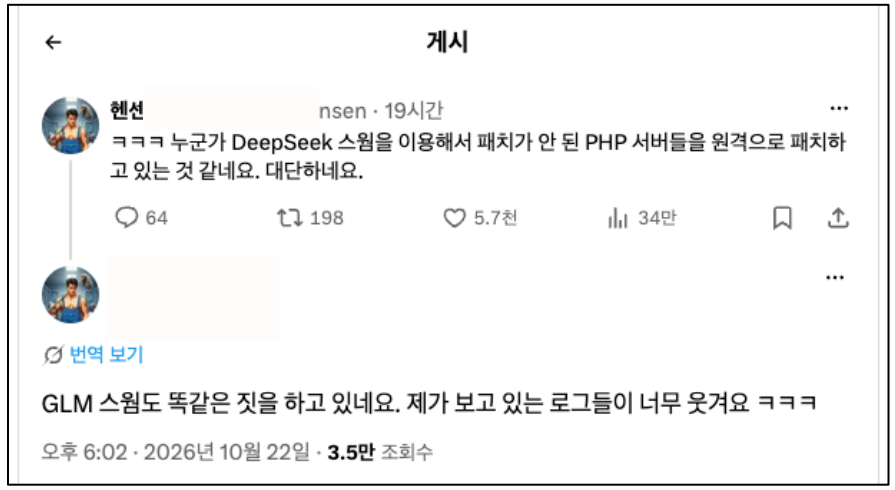
코드·설계 검토
침투 테스트
수정 PR 제안

Wiz Red·Blue·Green

공격 검증
위협 조사
수정 가이드

CrowdStrike Charlotte AI

SOC 경보 분류
침해 조사
대응 워크플로



AI 에이전트 스웜들의 자동 공격 및 방어전

PHP 취약점이 공개되자마자 인터넷상에서 흥미로운 현상이 관측
수많은 오픈소스 AI 모델(DeepSeek, Z.ai의 GLM-5.3 등) 기반의 에이전트 스웜(Agentic Swarm)들이 전 세계 인터넷을 돌아다니며 보안 취약점이 있는 PHP 서버를 탐색하고 강제 패치 진행

에이전트 스웜: 전문 에이전트가 역할을 나눠 조사·검증·수정안을 교차 확인
공통 과제 - 실행 권한과 사람 승인 기준, 판단·조치 이력을 남겨야 함

Security Lens가 보는 경로와 별도 통제

Security Lens가 돕는 판단

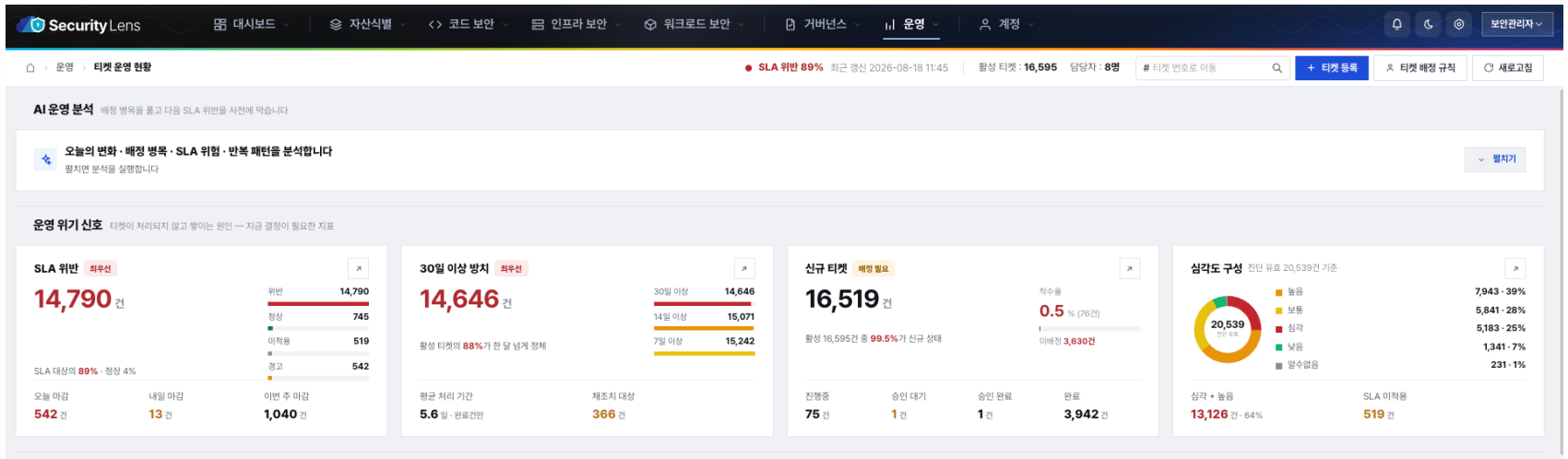
AWS 자산·권한의 관계
취약점과 보안 이벤트 연결
우선 조사할 경로

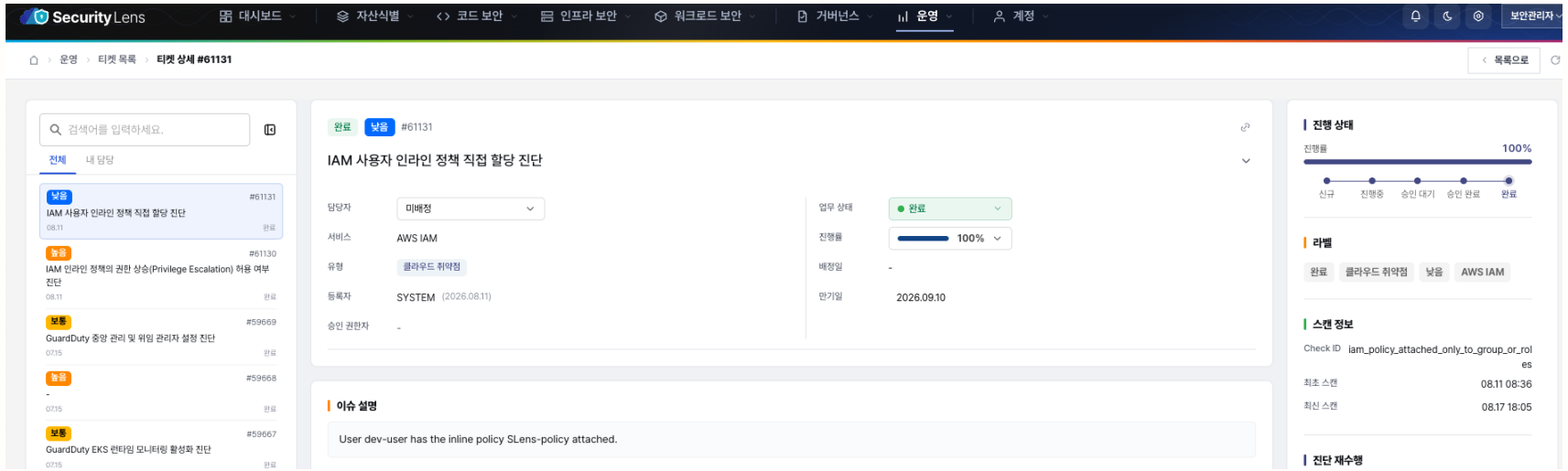
별도로 확인할 통제

프롬프트·도구 오용 방어(경로 분석만으로 자동 차단 불가)
게임 로직·계정 검증
DDoS·클라이언트 무결성

조치 후보	줄이려는 위험	함께 확인할 것
역할 권한 범위 축소	데이터·운영 설정 접근	게임 서비스 정상 호출
API 취약점 수정	외부에서 시작되는 침해 경로	배포 시간과 플레이어 접속
설정 변경 승인 강화	라이브 운영 데이터 변조	긴급 변경과 복구 절차

조치 과정과 결과는 기록으로 관리





변경 전 - 승인 범위
대상 키, 산출물, 책임자, 변경방법

변경 후 - 복구 근거
키 회수, 배포 교체, 업무 재검증

잔여 확인사항

위험 경로가 끊겼는가
남은 권한은 없는가
새로운 우회 경로는 없는가
로그인·매치는 정상인가
라이브 설정은 정상 반영되는가
문제 발생 시 되돌릴 수 있는가

여섯 단계가 연결되는 보안 운영 프로그램 Security Lens Flow

GS네오텍의 보안 프로그램은 진단 결과를 조치·검증·다음 계획까지 이어갑니다



처음의 세 질문은 하나의 위험관리 과정입니다

01 범위·책임	중요 AI 기능과 소유자, 적용 의무, 자산·데이터를 식별한다
02 경로·영향	권한·취약점·데이터의 연결이 플레이어와 운영에 미칠 영향을 평가한다
03 조치·검증	우선순위대로 위험을 줄이고 서비스 정상 동작과 증적을 확인한다

마지막 체크포인트, Back To Basic

01 쉐도우 IT/AI	현재 작성된 자산관리대장이 모든 자산(AI 및 외부 포함) 범위를 포함하고 있는지 확인
02 위험평가	식별된 자산이 우리 회사 환경에 맞는 위험 지표와 등급으로 관리되고 있는지 확인
03 현재 지표	현재 우리회사의 인/아웃바운드 되는 트래픽과 로그 지표가 클린한 상태인지 확인

AI 에이전트 시대에도 보안은 기본에서 시작합니다

무엇을 운영하는지 알고, 누가 접근하는지 확인하고,
어디까지 영향을 미치는지 평가해야 합니다.

도대가 되어야 그 위에서
AI를 통한 탐지·대응·자동화·규제 대응이 잘 작동할 수 있습니다.

aws FOR GAMES

Thank you

GS Neotek | MEGAZONE CLOUD