정보보호최고책임자 우수사례집
Best Practices of CISO

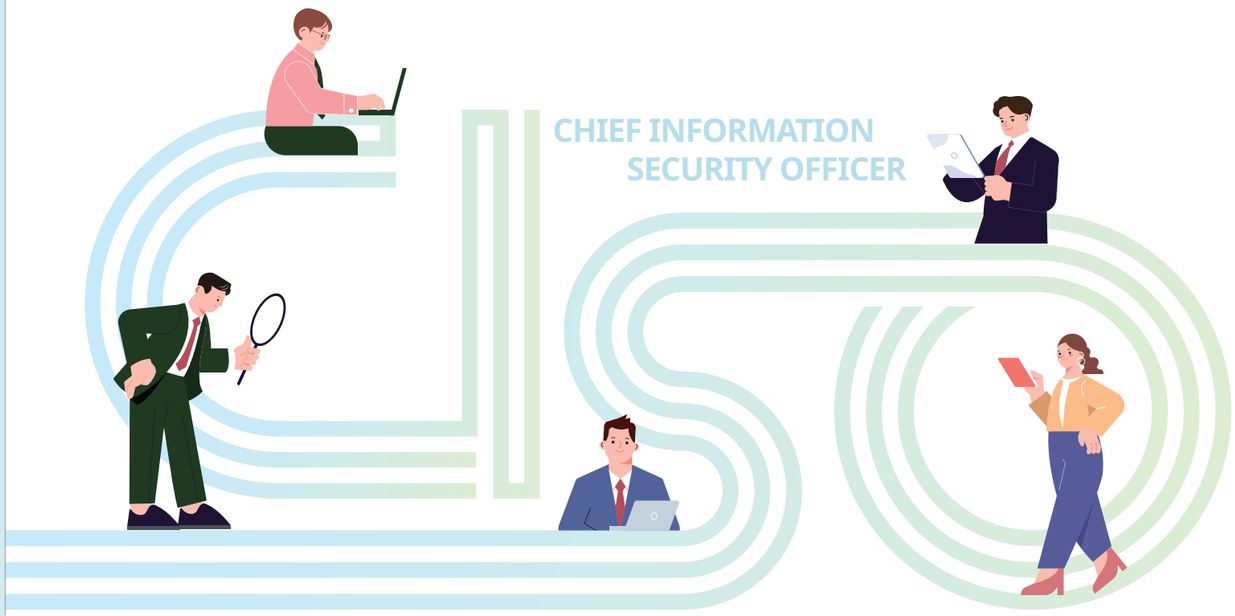
과학기술정보통신부

KISA 한국인터넷진흥원

2025.12

정보보호최고책임자 우수사례집

Best Practices of CISO



과학기술정보통신부

KISA 한국인터넷진흥원

2025.12

정보보호최고책임자 우수사례집

Best Practices of **CISO**

Encar | LOTTE WORLD

하나은행 | HYUNDAI GLOVIS | KZ 고려아연

과학기술정보통신부

KISA 한국인터넷진흥원

정보보호최고책임자
우수사례집

Best Practices of **CISO**

정보보호최고책임자(CISO) 지정·신고 제도는
민간 기업의 정보보호 투자확대 및 보안 역량 강화를 위한 제도입니다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3에 의거하여 정보통신서비스제공자는 정보보호최고책임자를 지정하고 과학기술정보통신부 장관(중앙전파관리소장에게 위임)에게 신고해야 합니다.

정보보호최고책임자 신고 의무대상은 자본금이 1억원을 초과하는 중기업 이상이면서 전기통신 역무(홈페이지 운영 등)를 이용하여 정보를 제공·매개하는 자가 해당됩니다.
- 전기통신사업자, 통신판매업자, ISMS인증의무대상자, 개인정보처리자 등

정보보호최고책임자는 사업주 또는 대표자, 이사, 정보보호 관련 업무를 총괄하는 부서의 장 이상으로 지정 후 신고해주시면 되며, 더 자세한 사항은 “정보보호최고책임자(CISO) 지정신고 제도 안내서” 또는 중앙전파관리소 홈페이지(https://www.crms.go.kr)를 참고 부탁드립니다.
* 홈 > 업무안내 > 방송통신사업 등록관리 > 정보보호최고책임자 지정·신고

정보보호최고책임자란?

정보보호최고책임자(CISO)는 기업의 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리 등 정보보호 업무를 총괄하는 최고책임자(CISO, Chief Information Security Officer)를 말함

- 정보보호최고책임자는 정보통신망법 제45조의3제4항 각 호에 따른 정보보호 관련 업무에 대한 최종 결정권 및 책임, 정보보호 업무관련 예산·인사에 대한 직접적 권한을 가짐

1. 정보보호최고책임자는 어떤 업무를 하나요?

- **(정보보호 계획의 수립·시행 및 개선)** 정보통신망의 안정성·신뢰성 확보를 위하여 관리적, 기술적, 물리적 보호조치를 포함하는 종합적 관리계획의 수립·시행 및 개선
- **(정보보호 실태와 관행의 정기적인 감사 및 개선)** 정보보호 실태 등에 대하여 조사하거나 관계 대상자로 부터 보고를 받을 수 있으며 정기적인 감사를 통해 사업주 또는 대표자에게 조사결과 및 개선조치를 보고
- **(정보보호 위험의 식별·평가 및 정보보호 대책 마련)** 하드웨어 또는 소프트웨어의 결함이나 체계 설계상의 허점으로 인해 사용자에게 허용된 권한 이상의 동작이나 허용된 범위 이상의 정보의 열람·변조·유출을 가능하게 하는 약점(취약점) 및 위험의 식별평가, 위험을 처리하기 위한 보안조치 설계, 정보보호 대책 마련
- **(정보보호 교육과 모의훈련 계획의 수립 및 시행)** 정보통신서비스 제공자를 대상으로 정보보호를 위해 최소 연 1회 이상 필요한 교육 및 침해사고 모의훈련을 실시

지정·신고 제도에 따른 대상자 구분

- **정보보호최고책임자(CISO) 지정·신고 기준은 기업유형 및 규모 등에 따라 차이가 있음**
- **신고의무가 제외된 기업은 별도 지정·신고 행위가 없는 경우 영 제36조의7제3항에 따라 사업주나 대표자를 정보보호최고책임자로 지정한 것으로 간주하여 정보보호 공백을 방지**

신고의무 제외대상
- 자본금 1억원 이하인 자
- 중소기업기본법 제2조제2항에 따른 소기업
- 전기통신사업자, ISMS의무대상자, 개인정보처리자, 통신판매업자 중 어느 하나에 해당하지 않은 중기업 정보통신서비스 제공자

→ **사업주** 또는 **대표자**

일반신고 의무대상
- (신고의무 제외대상에 해당하지 않은) 중기업 이상의 정보통신서비스 제공자
  - ★ '정보통신서비스 제공자'로서 '전기통신사업자, ISMS의무대상자, 개인정보처리자, 통신판매업자'는 CISO를 지정·신고하여야 함

→ **부서의 장** 이상

겸직금지 의무대상
- '정보통신서비스 제공자'로서 ①직전 사업연도 말 기준 자산총액 5조원 이상 또는 ②정보보호 관리체계(ISMS) 인증의무대상자 중 직전 사업연도 말 기준 자산총액 5천억 원 이상

→ 상법 상 **이사**

일반 자격요건 (정보통신망법 시행령 제36조의7제4항)

- **정보보호최고책임자는 임직원급으로서 다음 중 어느 하나의 자격요건을 갖추어야 함**

석사 학위* 이상 (정보보호·정보기술)	학사 + 3년 경력** (정보보호·정보기술)	전문학사 + 5년 경력 (정보보호·정보기술)	정보보호·정보기술 업무경력 10년이상	정보보호 관리체계 인증심사원 자격	정보보호 부서***의 장 근무경력 1년이상

* 정보보호 또는 정보기술 분야 학위란 전자 관련 학과, 정보통신 관련 학과, 정보보호 또는 정보처리기술 관련 학과의 과정을 이수·졸업한 학력을 의미함

** 정보보호 관련 업무는 정보보호를 위한 공통기반기술, 시스템·네트워크 보호, 응용서비스 보호 업무 등을, 정보기술 관련 업무는 정보통신서비스, 정보통신기기, SW 및 컴퓨터 관련 서비스 업무 등을 말함

*** 부서란 부, 팀 등 명칭과 관계없이 정보보호 업무를 담당하는 책임자와 담당자 등으로 구성된 조직을 말하며 장이란, 해당 조직의 책임자를 말함 (경력은 합산하여 산정)

겸직금지 대상기업 가이드라인

지위기준

① **정보보호최고책임자의 직위** (정보통신망법 시행령 제36조의7제1항)

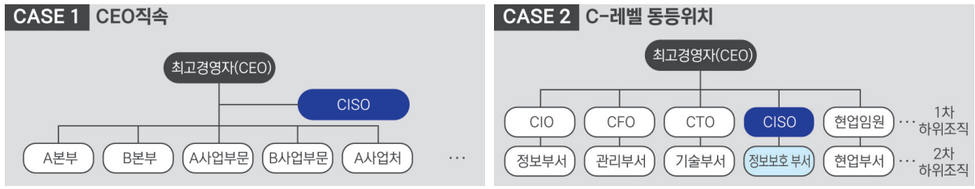
- 겸직금지에 해당하는 대상기업은 **이사**(상법 제401조의2제1항제3호에 따른 자 또는 같은 법 제408조의2에 따른집행 임원 포함)**로 정보보호최고책임자를 지정**해야 함

② **정보보호최고책임자의 지위**

- 정보보호최고책임자의 지위는 형식적인 직위가 아니라 정보통신망법 제45조의3제4항 각 호의 **정보보호 업무를 실질적으로 책임지는 자**를 의미
- **'대내외적으로 인정 될 만한 이사급 호칭을 사용'** 하고 **'실질적 의사결정'**을 종합적으로 확인

모범사례

- **(이사급 호칭)** 전무·상무(보)·이사·본부장·처장·임원 등 **대내외적으로 인정될 만한 이사급 호칭**을 사용
- **(실질적 의사결정)** 다른 임원과 직무상 독립하여 권한과 책임을 가진 자를 지정하여야 한다는 점을 고려하여 **CEO 직속** 또는 **다른 C-레벨과 등등한 위치를 가지는 정보보호 조직·위임전결을 가져야 함**
- **(조직체계 예시)**



위반사례

- **팀장·파트장·부장·차장·책임** 등 임원이 아닌 일반 직원에게 부여되는 호칭을 사용하고 있음
- 조직구성에 따른 직급제계와는 달리 **특수한 호칭**(센터장·실장·국장 등)을 부여하고 있으나, **실질적 정보보호 집행권한이 있다고 판단하기 어려운 경우**

ex) CEO 직속이 아닌 2차 하위조직으로 운영 or CEO 직속이지만 팀 단위(전체 조직도와 비교)로 판단되는 경우

겸직금지 운영기준

- 망법 상 겸직금지는 직위에 대한 겸직 금지가 아니라, **업무에 대한 겸직금지에 해당**
- 관련근거(정보통신망법 제45조의3제4항제1호, 정보통신망법 45조의3제4항제2호)에 따라 **'정보보호관련 업무'로 규정된 업무 외의 다른 업무는 겸직하지 않는 것이 원칙**

겸직가능 업무

- ① **정보보호 공시에** 관한 업무, ② **정보통신기반보호법**에 따른 정보보호책임자 업무, ③ **전자금융거래법**에 따른 정보보호최고책임자 업무, ④ **개인정보 보호법**에 따른 개인정보 보호책임자 업무, ⑤ 그 밖에 이법 또는 관계법령상 업무로서 정보보호최고책임자의 업무와 유사한 업무

※ ⑤는 직무·직위기술서, 조직도 등 CISO 조직이 망법에서 규정하는 업무를 전담하고 있는지 여부를 종합적으로 확인

위반사례

- **'대표이사', '경영기획·운영', '디지털(데이터) 전략기획', 'ICT기획·운영', '진료업무'** 등을 겸직

특별 자격요건 (정보통신망법 시행령 제36조의7제6항)

- 정보통신서비스 제공자가 **정보보호의 전문성을 갖춘 정보보호최고책임자를 임명**할 수 있도록 자격요건 규정
- 지정·신고 의무대상의 정보보호최고책임자는 일반 자격요건을 갖추어야 하고, **겸직금지 대상 정보보호최고책임자는 일반 자격요건과 특별 자격요건을 함께 갖추어야 함**
- 겸직금지 대상의 정보보호최고책임자는 일반 자격요건을 충족하고 상근하는 자로서, 다음 중 어느 하나에 해당하는 특별 자격요건을 추가로 갖추어야 함

상근 날마다 일정한 시간에 출근하여 정해진 시간동안 근무하는 것을 말함

출근 사회상규 상 해당 임직원의 근무장소, 사무공간, 사무용 자산 등에 지배력이 있는 상황에서 근로서비스를 제공하기 위한 근로 준비가 완료된 상태를 의미

정보보호 분야 업무경력이 4년이상 OR **정보보호 분야 업무경력과 정보기술 업무경력을 합산한 기간이 5년 이상** (2년 이상은 정보보호 분야 업무경력 필요)

* 정보보호 분야 업무와 정보기술 분야 업무를 동시에 수행한 경우에는 정보보호 경력으로 산정

정보보호최고책임자
Best Practices of CISO **우수사례집**

CONTENTS

Encar

엔카닷컴(주)

생성형 AI를 이용한 자동화된 취약점 점검 및 최신 취약점 보고 시스템 구축

기업 개요

설립연도	2014년
주요사업	온라인 중고차 플랫폼 회사
임직원 수	458명
정보보호 조직	정보보안팀(8명, CISO 포함)
기업 특성	엔카닷컴은 고객이 온라인에서 차량을 편리하게 사고 팔 수 있는 중고차 플랫폼 회사로써, 여러 가지 보안 위협으로부터 고객이 늘 안전하게 서비스를 이용할 수 있도록 하는 것이 필수 과제입니다.

추진 배경

엔카닷컴은 온라인에서 차량을 편리하게 사고 팔 수 있는 중고차 플랫폼 회사로써, 여러 가지 보안 위협으로부터 고객이 늘 안전하게 서비스를 이용하실 있도록 2014년부터 ISMS 인증을, 2019년부터 ISMS-P 인증을 받아오고 있습니다.

- **엔카닷컴은 2021년부터 총 4년간에 걸쳐 IDC에 있는 모든 서버를 AWS 클라우드로 이전하고 MSA (Microservice Architecture)를 도입하는 디지털전환을 성공적으로 수행하였는데, 그 결과로 클라우드 상 취약점 점검 대상 수가 2025년 8월 기준으로 총 923개로 급격하게 증가하였습니다.**
- **또한, 2022년부터 최근 3년간 신규 CVE 증가 추세를 보면 연평균 약 28,000건의 새로운 위협이 생겨나고 있습니다.**

이토록 취약점 점검 대상이 기하급수적으로 늘어나고, 날마다 신규로 생성되는 CVE에 대한 조사와 보고는 보안 담당자들의 업무 부하로 이어졌습니다. 이러한 상황 속에서 CISO로써 생성형 AI를 이용한 완전한 업무 자동화를 이뤄 보안담당자의 업무 부하를 줄이고 리소스를 전환하여 실질적인 보안 업무에 집중할 수 있도록 해야만 했습니다.

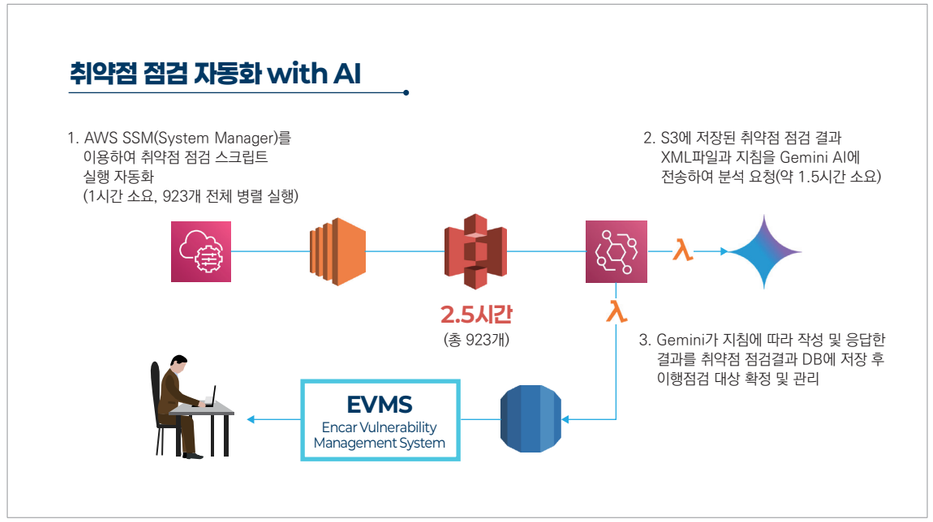
추진 내용 및 경과

① 생성형 AI를 이용한 자동화된 취약점 점검 시스템

과거 취약점 점검은 인프라 담당자가 총 923개의 취약점 점검 대상에 일일이 접속하여 점검 스크립트를 직접 수행하고 그 결과 파일을 생성하였는데 해당 작업에는 총 1.25개월이 소요되었습니다. 생성된 결과 파일은 정보보안 담당자에게 전달되었고, 결과파일을 전달 받은 보안 담당자는 결과파일을 하나씩 확인해 가며 수기로 보고서를 작성하였습니다. 보고서 작성에는 약 2달이 소요되었습니다. 보고서 작성이 완료되면 이행점검 대상을 확정하고 취약점에 대한 조치 및 관리를 하였습니다.

이렇게 총 3.25개월이 걸리는 취약점 점검 작업을 AWS SSM(System Manager)와 생성형 AI인 Gemini를 이용하여 완전히 자동화 시키는 것에 성공하였습니다. 자동화된 취약점 점검 시스템에서는 AWS SSM을 이용하여 총 923개의 점검 대상에 대한 점검 스크립트를 자동으로 동시에 병렬로 수행하게

하고 그 결과파일 역시 자동으로 생성하여 S3에 업로드 시키도록 하였습니다. S3에 적재된 취약점 점검결과는 AWS EventBridge와 Lambda를 통해 AI인 Gemini에 전달되고 Gemini는 사전에 작성된 취약점 결과 분석 지침에 따라 결과를 분석하고 분석결과를 응답합니다. 응답된 분석결과는 취약점 점검결과 데이터베이스에 영구 저장되어 EVMS(Encar Vulnerability Management System)에 의해 지속적으로 조치 및 관리되게 됩니다.

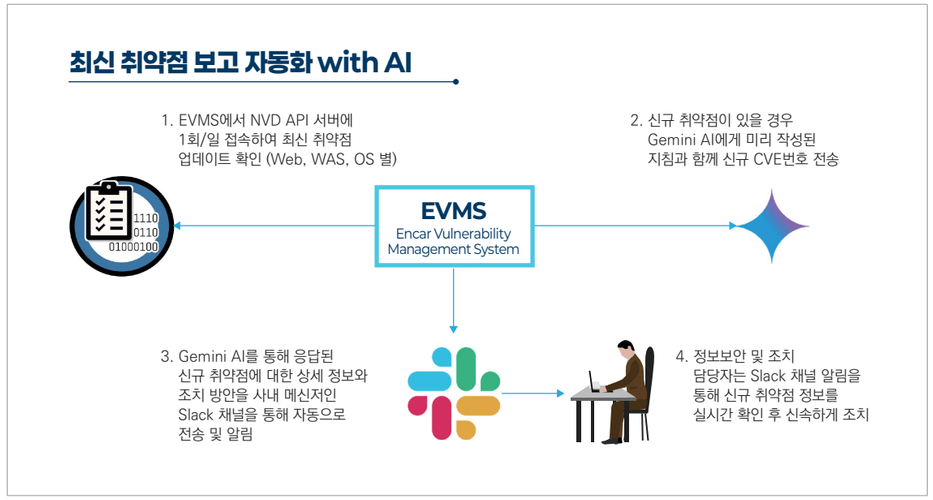


② 생성형 AI를 이용한 자동화된 최신 취약점 보고 시스템

과거 취약점 보고는 정보보안 담당자가 일별로 최신 취약점 정보 제공 사이트에 직접 접속하여 신규 취약점을 확인하고 신규 취약점이 있을 경우 조치 방안에 대한 리서치와 조치안을 마련 후 조치 담당자에게 이메일을 발송하여 조치를 요청하는 프로세스 였습니다.

이러한 최신 취약점 보고 프로세스를 NVD API와 생성형 AI인 Gemini를 사용하여 완전히 자동화된 시스템으로 구축하였습니다. EVMS(Encar Vulnerability Management System)는 최신 취약점 목록을 제공하는 NVD API에 자동으로 매일 접속하여 최신 취약점 목록을 확인 합니다.

만약 신규 취약점이 있을 경우 EVMS는 AI인 Gemini에게 미리 작성된 지침과 함께 신규 CVE번호를 전송합니다. Gemini는 전송된 CVE번호를 지침에 맞게 분석 후 신규 취약점과 조치방법에 대한 상세 정보를 규격화된 문서로 응답합니다. 이렇게 AI를 통해 분석된 취약점 정보는 사내 메신저인 Slack 채널을 통해 정보보안 및 취약점 조치 담당자에게 실시간으로 전송되어 담당자들이 실시간으로 신규 취약점을 확인하고 조치할 수 있게 되었습니다.



추진 성과

① 생성형 AI를 이용한 자동화된 취약점 점검 시스템

생성형 AI를 이용한 자동화된 취약점 점검 시스템 구축을 통해 기존 480시간(3.25개월)이 걸리던 취약점 점검 시간이 단 2.5시간으로 99.84% 단축 되었습니다. 이를 통해 취약점 점검에 들어가던 정보보안 리소스를 연간 약 65일 절감할 수 있게 되었습니다. 취약점 점검 시간이 단축됨에 따라 전체 대상에 대한 일별, 월별, 상시(긴급) 점검이 가능하게 되어 'BPFDoor' 이슈가 발생 했을 때에도 전체 긴급 점검을 수월하게 수행할 수 있었습니다. 또한 전 과정의 완전한 자동화를 통해 기존 수작업으로 인해 발생할 수 있었던 누락 및 보고서 작성 시 실수를 사전에 예방할 수 있게 되었습니다.

② 생성형 AI를 이용한 자동화된 최신 취약점 보고 시스템

생성형 AI를 이용한 자동화된 최신 취약점 보고 시스템 구축을 통해 기존 하루 1시간이 걸리던 취약점 보고 시간이 3분 이내로 95% 단축되었습니다. 이를 통해 취약점 보고에 사용되던 정보보안 리소스를 연간 10일(25년 근무시간 기준) 가량 절감할 수 있게 되었고, 근무일에만 가능하던 최신 취약점 보고를 자동화된 시스템을 통해 휴일 포함 365일 자동으로 수행할 수 있게 되었습니다.

이처럼 "생성형 AI를 이용한 자동화된 취약점 점검 및 최신 취약점 보고 시스템 구축"으로 인해 연간 사용되는 정보보안 리소스를 약 75일 절감하여 보안 담당자가 '모의해킹', '사전 보안성 검토', '이메일 대응 모의훈련', '보안 솔루션 실시간 모니터링' 등과 같은 실질적인 정보보안 업무에 집중할 수 있도록 하였습니다.

향후 계획 및 기대성과

앞으로 정보보안 업무에 AI를 보다 적극적으로 도입하고 추진할 계획입니다. '취약점 점검 이후 조치까지에 대한 자동화', '모의해킹', '사전 보안성 검토', '보안 솔루션 실시간 모니터링', '이메일 대응 모의훈련 자동화' 등 모든 정보보안 업무 영역에 AI를 통한 자동화를 적용하고 도입하여 정보보안 담당자들의 업무 효율을 더욱 올리고 실제 집중해야 할 보안 업무들에만 집중하고 노력하여 세계 최고 수준의 Zero-Trust 보안 태세를 수립해 나갈 계획입니다.

CISO 인터뷰

Interview

김명주 CISO는
CISO로써, 사이버 공격의 도구로
악용되던 AI를 이제 정보보호의 최전선,
즉 자동화된 방어 수단으로 적극적으로
전환하여 활용해야 한다고 강조했습니다.
복잡해지는 IT 인프라와 방대한 고객
데이터를 효과적으로 보호하기 위해,
AI 기반의 자동화는 더 이상 선택이 아닌
필수라고 하였습니다.
이는 날마다 폭발적으로 증가하는 보안 위협과 취약점으로부터
고객 정보와 핵심 시스템을 안전하게 지켜내는 핵심 전략이며,
궁극적으로 이러한 전략이 미래의 제로 트러스트(Zero-Trust)
보안 체계를 온전히 확립해 나가는 중요한 방향이라고 제시하였습니다.

LOTTE WORLD

호텔롯데 롯데월드

AI 기반 보안 챗봇과 정보보호포털 연계를 통한 정보보안 업무혁신 및 대응역량 고도화

기업 개요

설립연도	1989년
주요사업	테마파크 운영, 호텔·리조트 사업, 엔터테인먼트 서비스, 고객 경험 기반 디지털 서비스 운영
임직원 수	1,000명
정보보호 조직	정보보안부문(5명, CISO 포함)
정보보호 예산	10억원
기업 특성	롯데월드는 연간 1,000만 명 이상이 방문하는 테마파크·호텔·온라인 플랫폼이 결합된 복합 엔터테인먼트 기업으로서, 고객정보·결제정보·출입통제·IoT·운영설비(OT)·온라인 채널이 동시에 운영되는 초융합 보안환경을 보유하고 있다. 특히 고객 접점이 많은 만큼 고객 신뢰 기반의 정보보호가 핵심 경쟁력이 되는 기업이다.

추진 배경

최근 글로벌 산업 전반에서는 디지털 전환이 급속도로 확산되면서, 기업의 운영 구조가 과거에 비해 훨씬 복잡하고 다층적으로 변화하고 있는 양상이 나타나고 있습니다.

다수의 기업들은 클라우드 전환, 모바일 기반 업무 확산, 협업 시스템 증가, 온라인 서비스 채널 확대 등으로 인해 IT·보안 환경의 경계가 사실상 사라지는 흐름을 경험해 왔으며, 그 결과 보안조직이 관리·통제해야 할 영역은 과거보다 광범위하게 확장되고 있는 상황이 지속되고 있습니다.

특히 최근의 사이버 위협은 공격자의 기술 고도화와 자동화가 결합되면서 공격 주기가 짧아지고, 단일 공격이 광범위한 확산으로 이어지는 특징을 띠게 되었습니다.

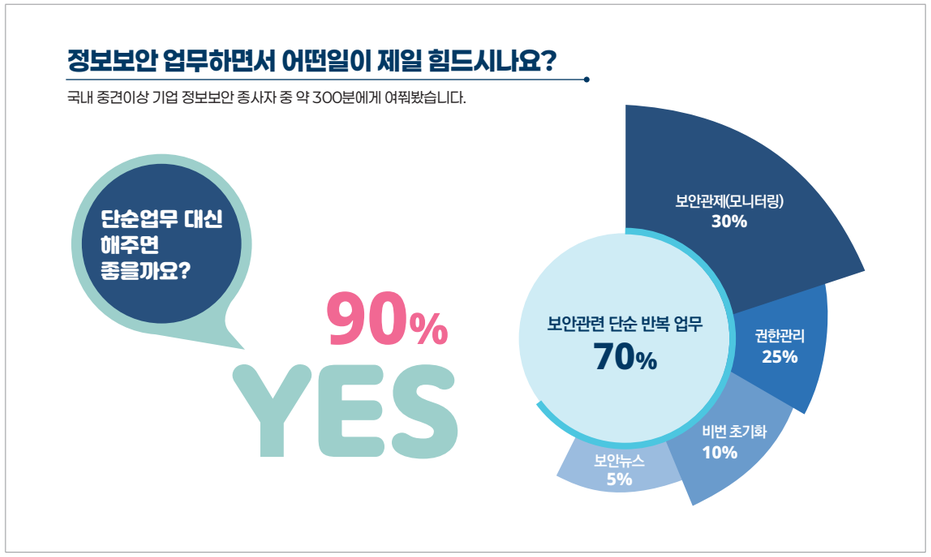
공격자는 AI와 자동화 스크립트를 활용하여 계정 탈취, 스피어피싱, 사회공학 기반 공격을 대규모로 수행하고 있으며, 위협의 정밀도 또한 향상되어 기업이 기존 방식만으로 대응하기 어려운 환경이 조성되고 있습니다. 이러한 변화는 산업군을 가리지 않고 모든 기업이 공통적으로 체감하고 있는 현실적 도전 과제가 되었습니다.

한편 기업 내부의 운영 방식도 혁신적 기술 도입이 빠르게 진행되면서, 구성원의 업무 패턴이 다양해지고 보안 절차에 대한 요구 수준도 과거보다 높아지는 방향으로 변화하였습니다. 업무 시스템이 복잡해지고 서비스 모델이 확장됨에 따라, 임직원이 보안정책·절차를 이해하고 이를 실제 현업에서 일관되게 준수하는 것이 어려워지는 사례가 다수 나타나게 되었습니다.

이에 따라 기업들은 구성원의 보안정책 문의에 신속하게 대응하고, 정책 해석의 불일치나 절차 준수의 편차를 최소화하기 위한 체계적 장치를 필요로 하게 되었습니다. 또한 다수 기업들은 보안조직의 역할이 단순 기술 운영을 넘어 전사 리스크 관리 기능을 수행하게 됨에 따라, 보안담당자의 의사결정 범위가 확대되는 현상을 경험하게 되었습니다. 반면 보안조직의 인력은 급격히 증가하기 어려운 구조적 특성이 있어, 증가하는 업무량 대비 인력·시간·자원의 한계가 누적되는 경향이 관찰되었습니다.

이러한 구조적 문제로 인해, 보안담당자가 반복적 운영업무에 과도한 시간을 투입하게 되면서 정작 고도화가 필요한 위협 분석·사고 예방·전략 수립 활동에 충분한 역량을 투입하지 못하는 현상이 여러 기업에서 공통적으로 나타나고 있습니다.

이와 더불어 많은 기업들이 정보보안 문서 작성, 이벤트 요약, 로그 분석, 계정 관리 등과 같이 반복적이고 정형화된 작업에 상당 시간을 사용하고 있어, 정보보호 운영의 효율성 향상을 통해 조직 전체의 사이버 대응 역량을 높여야 한다는 필요성이 갈수록 강조되고 있습니다.



특히 AI 기반 공격이 활성화되는 환경에서는 대응 체계 역시 동일하게 자동화·지능화를 통해 속도와 정확성을 확보해야 한다는 인식이 산업 전반에서 확산되었습니다.

이처럼 전 산업 분야에서 공통적으로 나타나는 업무 복잡도 증가, 보안 운영 부담 확대, AI 기반 공격의 고도화, 정책 문의·지원 증가, 보안조직의 역할 확장과 같은 흐름은 더 이상 개별 기업의 문제가 아닌, 모든 조직이 마주하고 있는 구조적 특징이자 시대적 과제입니다. 이에 롯데월드 역시 이러한 산업적 변화와 환경적 요구에 대응하기 위해 기존 보안 운영 모델만으로는 미래형 위협 대응 체계를 충분히 갖추기 어렵다고 판단하였습니다.

특히 보안담당자의 반복 업무를 효율화하고, 보안정책 준수도를 높이며, 이벤트 분석·보고 품질을 표준화하고, 위협 대응 속도를 획기적으로 향상시키기 위한 AI 기반 보안 혁신 모델의 필요성이 점차 명확해지게 되었습니다. 이와 같은 배경 속에서 롯데월드는 AI·LLM 기반 보안 챗봇, RPA 기반 자동화 체계, 그리고 API 연계를 활용한 보안 이벤트 자동처리 구조를 결합한 차세대 정보보안 업무혁신 프로젝트를 본격적으로 추진하였습니다.

추진 내용 및 경과

롯데월드는 정보보안 운영방식의 고도화를 위해 'AI 기반 보안업무 혁신 체계'를 구축하는 것을 핵심 목표로 삼고 단계적으로 추진을 진행하였다. 본 사업은 AI 기반 보안 챗봇 구축, 반복 업무 자동화(RPA), 보안 솔루션 API 통합 자동화, 조직 전체의 보안정책 준수도 향상, 보안 이벤트 분석·보고 체계 표준화라는 5가지 축을 중심으로 전개되었습니다. 각 세부 내용은 다음과 같습니다.

1. AI 기반 보안 챗봇(Security GPT) 기획

롯데월드는 보안담당자가 수행하던 반복적·문서 기반·지식 기반 업무의 상당 부분을 AI가 보조할 수 있도록 전용 LLM 기반 보안 챗봇을 기획 했습니다. 이는 단순 지식 검색 기능을 넘어, 실질적으로 보안조직의 의사결정을 지원하는 실무 도구로 설계되었습니다.

① 내부 보안 정책·절차 자동응답 체계 구현

롯데월드는 수년간 운영해온 보안정책, 개인정보보호 지침, 내부 규정, 실무 가이드, FAQ 등 방대한 텍스트 기반 자산을 구조화하여 챗봇 학습 데이터로 활용했습니다. 이를 통해 구성원의 질문에 대해 일관된 기준과 정확한 규정을 근거로 즉각적인 답변을 제공하는 체계가 마련되었습니다. 이를 통해 보안담당자가 수행하던 반복적인 정책 설명 업무가 크게 감소하였으며, 사용자는 언제든지 실시간으로 정책을 확인할 수 있게 되었습니다.

② 보안 인시던트 보고서 자동 초안 생성 기능 구현

LLM을 활용하여 탐지 이벤트, 로그 정보, 경보 설명 등을 입력하면 AI가 인시던트 초안을 자동으로 작성하도록 구현했습니다. 이로써 보안담당자는 내용의 사실 여부와 조치 방향만 검토하면 되어, 기존에 수십 분에서 수 시간이 소요되던 작성 절차가 수분 이내로 단축되었습니다.

③ 보안 이벤트 요약 및 대응 방향 추천 기능 구현

로그와 탐지 이벤트의 기술적 설명을 난이도에 맞춰 요약하고 유사 패턴 기반 대응 방향을 제시하도록 구성하였다. 기술 배경이 부족한 사용자나 경영진 보고 시에도 유용한 체계가 구축되었습니다.

④ 사용자 보안 문의 자동응답 시범 운영

VPN 오류, 기기등록, 계정잠김, 비밀번호 재설정 등 사용자 문의가 빈번한 영역을 중심으로 자동 응답을 제공하게 하였으며, 내부 인트라넷과 연동하여 간단한 절차는 직접 처리되도록 하였습니다.

2. API·RPA 활용한 보안업무 자동화

롯데월드는 보안담당자가 반복적으로 수행하는 '운영성 작업'을 자동화함으로써 조직 전체의 생산성과 보안 정확도를 높이고자 했습니다.

① 계정 라이프사이클 자동화

입사자·퇴사자·부서 이동에 따른 계정 생성·변경·삭제 절차를 자동화하였다. HR 시스템과 IAM 시스템을 연동하여 계정 처리의 누락이나 지연을 최소화하였고 보안 설정 편차가 사라지도록 자동 프로세스를 도입하였습니다.

② 권한 검토 및 정책 준수 점검 자동화

사용자별 권한 현황과 변경 이력에 대해 RPA가 자동으로 정리·검토하도록 구성하여 기존의 수작업 기반 프로세스에서 발생하던 작성 오류와 검토 누락이 감소했습니다.

③ 보안 로그 수집·정리 자동화

서버, OS, DB, 클라우드, 네트워크 장비 등 다양한 보안 로그를 자동 취합하여 주간·월간 보고서를 자동 생성하도록 구성했습니다.

④ 취약점 스캔 결과 리포트 자동화

취약점 항목 분류, 위험도 점수, 조치 필요 항목 등을 자동 정리하여 실무자의 분석 시간을 획기적으로 단축했습니다.

3. 보안 시스템 API 통합 자동화 기반 구축

롯데월드는 SIEM, EDR, IAM, DLP 등 주요 보안 시스템을 API 기반으로 연결하여 탐지 → 분석 → 조치 → 보고까지 자동 수행되는 구조를 단계적으로 구축했습니다.

① SIEM 기반 탐지 이벤트 자동 알림

SIEM에서 특정 패턴이 탐지되면 관련 메신저로 자동 전송되도록 구현하였다. 이를 통해 담당자의 탐지 확인 시간을 단축시키는 효과가 나타났습니다.

② EDR 기반 자동 격리 조치

EDR이 악성 프로세스 또는 의심 프로세스를 탐지하면 API를 통해 자동으로 격리 요청이 수행되도록 구성했습니다.

③ IAM 기반 비정상 로그인 자동 MFA 전환

로그인 위치·속도·시간대가 비정상적일 경우 IAM이 자동으로 MFA 인증을 요구하도록 했습니다.

④ SOC 티켓 자동 생성

탐지 이벤트가 기준치를 넘으면 JIRA 티켓이 자동 등록되도록 구현하여 누락 없는 사고대응 체계를 마련했습니다.

4. 보안 조직·전사 보안문화 강화 프로그램 운영

AI 기반 체계의 기술적 효과를 극대화하기 위해 조직·문화·교육·내부 커뮤니케이션 개선도 병행했습니다.

① 실무자 중심 보안 교육 체계 구축

사례 기반 모의훈련, 직무별 맞춤형 실습 프로그램을 제공하여 AI 기반 분석 결과를 실무에 바로 활용할 수 있도록 했습니다.

② 보안 정책 안내 콘텐츠 강화

카드뉴스, 인포그래픽, 단문 정책 안내 등을 제작하여 임직원 이해도를 높이고 정책의 접근성을 향상시켰습니다.

③ 협력사 보안 가이드라인 공유

협력사·파트너사 계정을 사용하는 경우가 많은 기업 특성을 반영하여 보안 준수 항목을 명확히 안내하고, 챗봇을 통해 기본 답변이 가능하도록 했습니다.

다음으로, 롯데월드는 AI 기반 보안운영 고도화를 추진하는 과정에서 전사 구성원들이 보안 정책을 보다 쉽게 이해하고 즉시 활용할 수 있도록 지원하기 위해 정보보호포털(Information Security Portal)을 신규로 구축했습니다. 기존에는 보안 정책, 가이드, 절차 안내, 문서 양식 등이 여러 시스템과 문서 저장소에 분산되어 있어 임직원이 필요한 정보를 찾는 데 시간이 걸리고, 설명 방식이 부서마다 달라 혼선을 유발하는 경우도 있었습니다. 이에 롯데월드는 보안과 관련된 모든 정보를 단일 창구에서 확인하고, 정책 안내·사고 신고·보안 요청·교육 이수 현황을 통합 관리할 수 있는 전사 정보보호포털을 구축하는 것을 주요 과제 중 하나로 설정했습니다.

추진 성과

롯데월드가 추진한 AI 기반 정보보안 업무혁신 프로젝트는 기술 도입의 단편적 성과를 넘어, 보안조직의 운영 방식·업무 처리 구조·사고 대응 체계·전사적 보안문화에 이르기까지 다양한 측면에서 실질적인 변화와 개선을 이끌어내는 결과를 나타냈습니다.

특히 반복 업무 자동화, 대응 속도 향상, 정책 준수도 증대, 사용자 만족도 개선 등 정량적·정성적 지표 전반에서 고른 성과가 도출되었습니다. 아래에서는 본 프로젝트를 통해 확인된 주요 성과를 정량적 성과와 정성적 성과로 나누어 상세하게 기술하였습니다.

1. 정량적 성과(Quantitative Outcome)

① 반복 업무 소요시간 대폭 절감 효과가 나타났습니다. AI 챗봇과 RPA 기반 자동화가 정착되면서 보안담당자가 기존에 수작업으로 처리하던 반복 업무의 부담이 획기적으로 줄어들었습니다. 정책 문의 대응, 계정 설정, 인시던트 초안 생성, 로그 정리 등 일상적이면서도 시간이 많이 소요되던 업무가 자동화되면서 전체 보안 조직의 업무 처리 속도가 크게 향상되었습니다.

- 보안 정책 문의 대응 시간 : 약 70% 감소
- 인시던트 보고서 초안 작성 시간 : 약 80% 단축
- 연간 절감된 반복 업무 시간 : 1,200시간 이상 절감 효과

이와 같은 절감 효과는 단순히 시간 단축에 그치지 않고 보안담당자가 전략적 업무에 시간을 투자할 수 있도록 구조적 변화를 시켰습니다.

② 보안 이벤트 대응 속도가 획기적으로 개선되었습니다. AI 챗봇과 API 자동조치 기능이 결합하면서 탐지 이벤트 확인부터 실제 대응까지 걸리는 전체 프로세스가 압축되어 이전에는 수 시간에서 반나절 이상이 소요되던 절차가 평균 15분 이내로 단축되는 개선 효과가 나타났습니다. 특히 다음과 같은 영역에서 성과가 두드러졌습니다.

- 보안 이벤트 탐지 → 조치까지 평균 처리시간 → 기존 평균 8시간 → 개선 후 15분 미만
- EDR 기반 자동 격리 성공률 → 98% 이상 안정적으로 유지
- 비정상 로그인 자동 MFA 전환 처리율 → 기존보다 약 40% 향상

이는 보안사고의 확산을 차단하는 데 결정적인 역할을 하였으며, 최초 대응의 신속성과 대응 품질의 일관성을 동시에 확보할 수 있게 했습니다.

③ 계정 기반 사고 및 운영 리스크가 실질적으로 감소되었다. 계정 권한 오남용, 비정상 로그인, VPN 오류 및 계정 잠김 등 계정 기반 이벤트는 대부분의 기업에서 빈번하게 발생하는 문제 중 하나였다. 롯데월드 역시 API 자동화·RPA·AI 기반 챗봇을 결합하여 계정 관련 이슈를 자동 감지·자동 조치하는 체계를 마련함으로써 관련 사고 발생률이 유의미하게 감소하는 결과를 얻었습니다.

- 비정상 로그인 대응 지연 건수 : 40% 감소
- 계정 삭제 지연(퇴사자 계정) : 지연 사례 0건 달성
- 권한 설정 오류 발생률 : 자동화 적용 후 크게 감소

이는 계정 기반 공격(credential-based attack) 비중이 높은 최근 위협 특성에 대응하는 데 중요한 개선 성과로 평가됩니다.

④ 전사적 보안정책 준수도가 눈에 띄게 향상되었습니다. AI 챗봇이 전사 구성원의 보안질문에 정확하고 즉각적으로 답변하게 되면서 정책 안내의 일관성과 접근성이 크게 높아졌다. 그 결과, 사용자의 정책 이해도·준수도가 자연스럽게 향상되는 효과가 나타났습니다.

- 정책 관련 문의 응답 시간 단축 → 정책 준수율 증가
- 정책 해석 편차 감소 → 절차 위반 건수 감소
- 문서 암호화·접근 권한 신청 등 각종 요청 절차 오류 90% 감소

기존에는 “정책을 잘 몰라서” 발생하던 준수 오류가 AI 챗봇을 통해 단기간에 감소되는 성과가 나타났습니다.

2. 정성적 성과(Qualitative Outcome)

정량적 성과 외에도, AI 기반 보안 혁신 프로젝트는 조직문화·업무 방식·의사결정 구조·대응 품질 등 정성적 측면에서 매우 큰 긍정적 변화가 확인하였습니다.

① 보안담당자의 업무 집중도가 크게 향상

반복 업무가 자동화되자 보안담당자들은 위협 헌팅·심층 로그 분석·보안 아키텍처 검토 등 전문성을

요구하는 업무에 충분한 시간을 투입할 수 있었습니다. 과거에는 단순 운영 업무에 대부분의 시간을 사용하였다면, 현재는 고위험 영역 중심의 분석 비중이 크게 늘어 조직 전체의 보안 대응력 수준이 눈에 띄게 개선되었습니다.

② 구성원의 보안 인식 및 정책 준수도가 자연스럽게 강화

AI 챗봇을 통해 항상 동일한 기준으로 정책 안내가 제공되면서 사용자의 보안 인식이 균일하게 강화되었고 정책 준수 의식이 전체적으로 향상되는 효과가 나타났습니다. 특히 “정책을 몰라서 발생하던 실수”가 현저하게 줄었으며, 보안팀이 직접 설명하는 대신 챗봇이 전담하게 됨으로써 정책 교육의 접근성과 지속성이 크게 개선되었습니다.

③ 보안조직에 대한 신뢰도와 경영진의 관심도 모두 증가

자동화·AI 기반 운영 성과가 명확히 나타나자 보안조직에 대한 전사적 신뢰도가 향상되었으며, 경영진 보고 품질도 크게 높아졌다는 평가가 이루어졌습니다. 보고서 자동 생성 기능, 이벤트 요약 기능 등을 통해 경영진은 기술적 내용을 쉽게 이해할 수 있게 되었고 보안 의사결정에 대한 대응 속도와 정확성이 함께 높아졌습니다.

④ 사고 대응 프로세스의 표준화가 이루어져 조직의 안정성 강화

AI 기반 분석 및 자동화 프로세스가 도입되자 사고 대응 절차가 개인 역량이나 상황에 영향을 받지 않고 일정한 품질로 운영되기 시작했습니다. 이는 보안 운영의 예측 가능성과 안정성을 크게 높였으며 사고 대응 실패 위험을 구조적으로 낮추는 결과를 가져왔습니다.

⑤ 보안팀과 현업 부서 간 커뮤니케이션 비용이 크게 감소

과거에는 보안 정책·절차 문의가 이메일·전화·메신저 등으로 산발적으로 발생하여 보안팀이 상당한 시간과 노력을 소비했습니다. AI 챗봇이 이를 전담하게 되면서 현업 부서의 질문 처리 속도가 빨라졌고 보안팀은 단순 대응에 시간을 소모하지 않아도 되는 구조가 만들어졌습니다.

종합적으로, 본 프로젝트는 운영 효율화·조직문화 변화·대응 역량 향상·경영진 신뢰도 제고 등 전사적 차원의 다층적인 성과를 창출했습니다.

향후 계획 및 기대성과

롯데월드는 이번 AI 기반 보안업무 혁신 프로젝트를 통해 확보한 기술적 기반과 운영 경험을 바탕으로, 향후 더욱 고도화된 AI 기반 위협 대응 체계, 전사 보안문화 강화 전략, 협력사 보안관리 확장 모델을 단계적으로 구축할 계획이다. 특히 최근 고도화되는 계정 기반 공격, 자동화된 침투 탐색, 내부자 이상행위 증가 등의 산업 환경 변화에 대응하기 위해 다음과 같은 구체적 실행 방향을 수립했습니다.

첫째, AI 기반 이상징후 탐지 체계 고도화

현재 운영 중인 API·LLM 기반 자동화 프레임워크 위에 사용자 행동 패턴(UBEA), 접속 위치·시간대 분석, 디바이스 리스크 점수화 등을 결합하여 비정상 로그인·세션 하이재킹·권한 오남용과 같은 위험 징후를 사전에 감지하고 자동으로 차단하는 기능을 강화하고자 한다. 이를 통해 “탐지 이후 대응” 중심의 구조를 넘어, “탐지 이전 예방” 중심의 선제 대응 모델을 구축할 수 있을 것으로 기대된다.

둘째, 보안자동화 범위를 전사 서비스 영역으로 확대

현재는 내부 운영 중심 업무자동화가 중심이지만, 향후에는 고객 서비스, 키오스크, 앱·웹 채널, 운영설비(OT) 등 테마파크 특성이 반영된 다양한 접점 영역까지 자동화 모델을 확장할 방침이다. 특히 부모·아이·외국인 방문객 비율이 높은 서비스 특성상 사용자 행태 기반 이상 행위 분석 모델 적용을 통해 보안 위협 조기 감지 효과를 높일 수 있을 것으로 기대된다.

셋째, 협력사·외주사 대상 보안관리 체계를 AI 기반으로 전환

협력사 계정 발급, 접근권한 검증, 접속 패턴 모니터링, 보안점검 이행 여부 확인 등을 자동화하고 보안 챗봇을 통해 협력사가 필요한 정책·절차를 즉시 안내받을 수 있도록 할 예정이다. 이를 통해 협력사 보안수준을 균등화하고 관리 부하를 줄이는 효과를 기대하고 있다.

넷째, 경영진 보고 및 의사결정 체계를 데이터 기반으로 고도화

현재 운영 중인 자동 요약·보고 기능을 더욱 고도화하여 이사회 보고서, CISO 주간보고, 사고보고서, 개선안 보고 등 다양한 문서 형식을 자동으로 생성·정리할 수 있도록 만들어 경영진이 사이버 리스크를 직관적으로 이해할 수 있는 환경을 마련하고자 한다.

다섯째, 롯데월드는 성공적으로 정착된 AI 기반 보안업무 모델을 기반으로 향후 타 계열사 및 유관 산업군과의 보안 협력 확대도 검토하고 있습니다. 테마파크·호텔·레저 산업은 고객 정보와 운영 정보가 동시에 존재하는 독특한 구조로 AI 기반 보안운영의 적용 효과가 특히 크다는 점에서 향후 본 사례가 관련 업종의 표준 모델로 자리매김 할 수 있을 것입니다.

CISO 인터뷰

Interview

주진국 CISO는 "CISO의 역할은 단순히 기술을 총괄하는 데 그치지 않고, 전사적 디지털 리스크를 조율하며 조직 전체가 보안 원칙을 자연스럽게 실천하도록 만드는 것이라고 생각한다.
이번 기획을 통해 롯데월드가 보안운영의 새로운 체계를 마련하게 된 중요한 계기가 되었으며, 기존에 수작업 중심이었던 운영 모델을 데이터 기반·AI 기반 의사결정 구조로 전환시키는 전환점이 되었다"고 전했다.

하나은행

㈜하나은행

지속적 다계층 보안 위험 관리 – 정보보호 영향도 평가

기업 개요

설립연도	1991년
주요사업	은행업
임직원 수	11,352명
정보보호 조직	정보보호본부(88명, CISO 포함)
정보보호 예산	464.5억원(2024년 집행액)
기업 특성	하나은행은 지난 50여년간 안전하고 편리한 금융서비스를 기반으로 '내일이 더 기대되는 은행'이라는 기업가치를 모토로 끊임없는 혁신과 신뢰를 기반으로 정보보호 안정성 보증 노력을 지속하고 있습니다.

추진 배경

대형 SI 개발 프로젝트에서 발생할 수 있는 정보유출, 침해사고, 규제 요구사항 미준수 등 다양한 내부·외부 보안 위협 발생에 대응하고자 프로젝트 전체 라이프사이클에 거쳐 **보안 위협 사전 관리 방안**을 마련했습니다.

기존의 위험평가 방법론이 갖는 최신 위협에 대한 변화 반영 부족, 업무 환경 변화 대응 및 규제 최신화 미흡 등의 한계를 극복할 수 있는 **"정보보호 영향도 평가" 방법론을 마련하여** 정보보호 위험을 동적으로 관리 가능하게 할 수 있습니다.

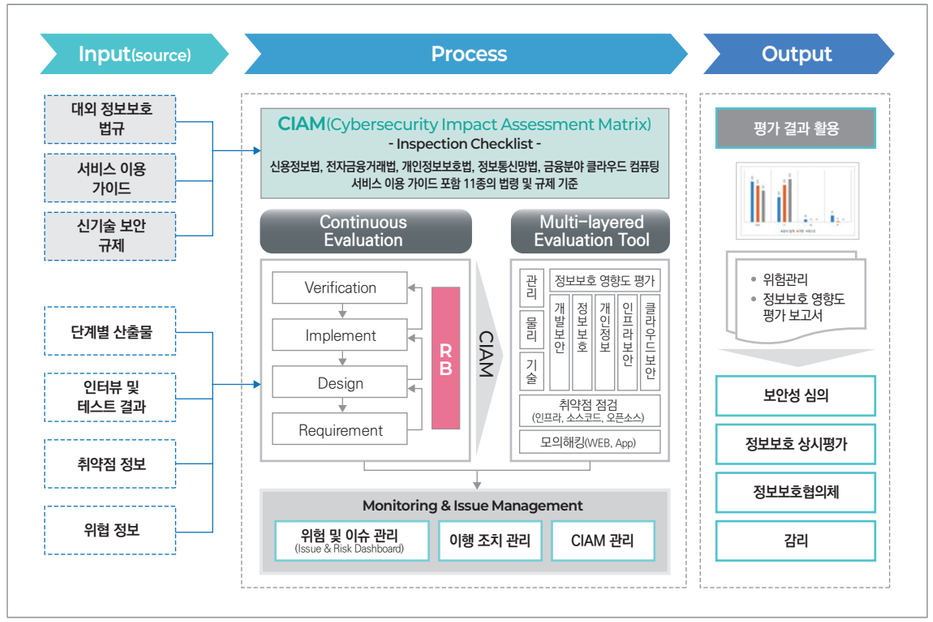
추진 내용 및 경과

추진 내용

(1) 정보보호 영향도 평가 개요

"정보보호 영향도 평가 방법론"은 지속적이고 다계층적인 보안 위험 관리 방법으로 프로젝트 계획시부터 종료시까지 프로젝트 결과물의 안전성 확보를 목표로 합니다.

〈정보보호 영향도 평가 Framework〉



(2) 정보보호 영향도 평가 절차

① 정보보호 영향도 평가 기준(체크리스트) 마련

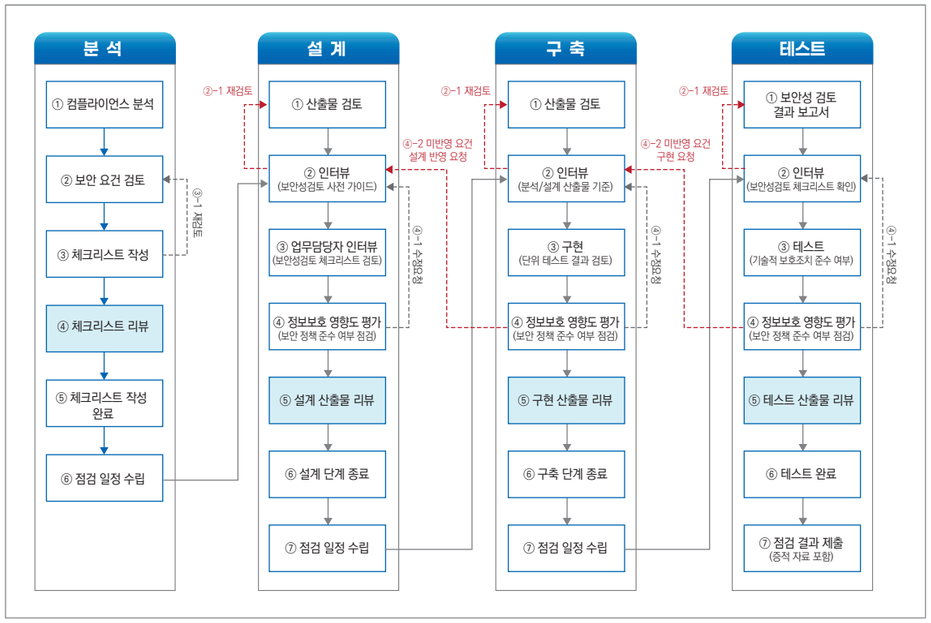
② 정보보호 영향도 평가 실시 계획 수립

③ 정보보호 영향도 평가 실시

④ 정보보호 영향도 평가 관리

- 사업 영역 x 평가항목 x 사업 단계별 = 점검 결과 관리
- 점검 결과 기반 피드백 관리를 통한 정보보호 안전성 향상
- 프로젝트 요구사항 변경 사항 발생시 정보보호영향도 점검

〈정보보호 영향도 평가 활용 프로세스〉



추진 경과

(1) '21년도 마이데이터 사업 정보보호 안전성 강화 방안 최초 적용

① 정보보호 무결점 시스템 구축 완료

② **정보보호영향도 평가 방법론 자체 마련 및 수행**

③ **금융그룹 관계사 확대 적용** → 마이데이터 사업 정보보호영향도평가 지원: 점검 항목 및 결과 공유

(2) ‘23년도 하나은행 프로젝트 O.N.E(Our New Experience) 사업 적용

정보보호영향도평가 적용을 통해 사전 식별하고 조치함으로써 미 식별된 보안 위험에 의한 **프로젝트의 전체 영향도 예방과 추가 소요될 비용을 절감함**

① 분석/설계 점검 대상 793건 적용 대상중 N/P 358건 식별 → 331건 선조치

② 구현단계 점검 대상 1,131건중 N/P 27건 식별 → 27건 선조치

③ 테스트단계 점검 대상 1198건 N/P 0건 → 분석/설계/구현 단계 선조치 완료

(3) ‘25년도 하나은행 프로젝트 FIRST 사업 적용 진행중

(4) ‘25년 4월 정보보호영향도 평가 수행 절차 가이드 발간

(5) ‘25년 6월 정보보호영향도 평가 **특허 출원**

출 원 번 호 통 지 서

출 원 일 자	2025.06.20
특 기 사 항	심사청구(무) 공개신청(무) 참조번호(DP25144)
출 원 번 호	10-2025-0082135 (접수번호 1-1-2025-0696435-93) (DAS접근코드3BBE)
출원인 명칭	주식회사 하나은행(1-1998-096852-9)
대 리 인 성 명	특허법인
발 명 자 성 명	
발 명 의 명 칭	정보보호 영향도 평가 방법 및 그 장치

추진 성과

(1) 분석/설계 단계부터 보안 내재화 수행, 보안 위험 사전 식별 및 점검으로 정보보호 안전성 확보 → **정보보호 무결점 시스템 구축 완료**

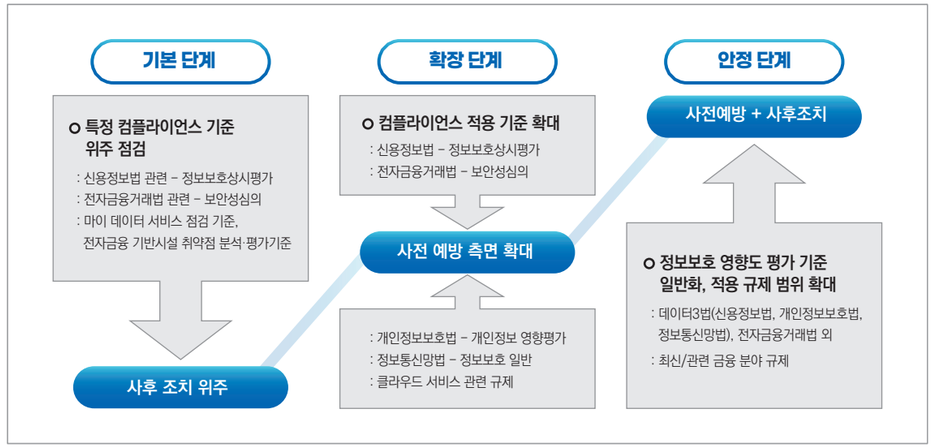
(2) 프로젝트 초기부터 보안을 고려 하여 장기적으로 개발 비용 절감하고 효율적 정보보호 정책 구현 → **최소의 비용으로 프로젝트 안정성 및 효율성 확보**

향후 계획 및 기대성과

(1) “정보보호영향도 평가” 방법론 지속 발전

(2) “정보보호영향도 평가” 금융 정보보호 수준 평가 표준 기준으로 활용

(3) 금융 정보보호 위험 관리 방법론으로의 활용



CISO 인터뷰

Interview

방명환 CISO는

“정보보호 영향도 평가를 대형 프로젝트에 적용해보는 시도가 프로젝트를 지연시키는 요소로 작용할 우려도 있었지만, 프로젝트 초기단계부터 보안 취약 요소를 점검하고 보완하면서, 실제로 조직의 전반적인 정보보호 레벨이 개선되는 효과로 이어져 뿌듯함을 느꼈다”고 전했습니다.

현대글로비스(주)

정보보호 거버넌스 체계 확립

기업 개요

설립연도	2001년
주요사업	유통, 물류, 해운
임직원 수	1,900명
정보보호 조직	정보보호담당(12명, CISO 포함)
정보보호 예산	57.3억원(2025년 정보보호 공시 기준)
기업 특성	현대글로비스는 최첨단 IT시스템 구축을 통한 물류 전 과정에 대한 서비스를 제공하는 Global Top Tier SCM 전문 기업으로서 공급망 전반 보안 수준을 강화하고 AI, 머신러닝, 클라우드 등 최신 보안 위협에 대응하는 것이 주요 과제입니다.

추진 배경

공급망 보안은 단순히 IT시스템을 보호하는 수준을 넘어 기업의 비즈니스 연속성과 신뢰성을 유지하는 핵심 요소로 자리 잡고 있습니다. 현대글로비스는 이러한 사이버 위협 환경 변화를 감안하여 2025년 CISO 조직을 개편하고 정보보호 추진전략 및 로드맵을 수립하여 공급망 전반 보안 수준 강화를 위해 체계적으로 정보보안 업무를 수행하고 있습니다.

추진 내용 및 경과

현대글로비스는 현대자동차그룹 차원의 “SRE(Site Reliability Engineering)” 활동을 2023년부터 추진해 오고 있습니다. 이 활동은 全 그룹사 및 해외법인에 대한 보안/ICT KPI 평가제도를 운영함으로써 그룹의 지속적인 보안 수준 향상을 도모하고 안전한 비즈니스 환경을 보장하는 것이 핵심입니다. 또한 그룹 보안정책 협의회를 매월 개최하여 현대자동차그룹의 보안수준을 점검하고, 표준보안 솔루션을 선정 및 구축하는 등 공통된 정보보호 정책으로 국내/외 확산 전개하고 있습니다. 추가적으로 정보보호 추진전략의 신속한 이행을 위해 보안조직을 팀단위에서 실급 조직으로 신설하였으며 정기적인 경영층 보고체계를 마련하여 전략 로드맵에 따른 TOP-DOWN식의 효과적인 보안과제 수행을 위한 토대를 마련하였습니다. 이와 병행하여 실질적인 사고예방 및 인식제고 프로그램을 운영함으로써 보안수준 향상을 더욱 극대화 하고 있습니다.

① 경영진의 보안에 대한 관심과 참여를 유도하기 위해 CISO는 연 2회 정기 이사회에서 정보보안 현황과 리스크를 보고합니다. 아울러 경영층 대상 조직별 분기 KPI 중간 점수를 공유하여 보안에 대한 경각심을 고취하고 있습니다. 각 팀별 지정된 보안담당자를 대상으로 정보보안협의회를 수행하여 보안 유의사항 전파, 보안업무 수행 요청을 통해 회사 전반의 책임감을 함께 높이고 있습니다. 또한 국내/외 보안사고 발생 시 그룹 통합보안센터 주관 당사의 현황을 사전 점검하고 수시 보고하여 사고를 미연에 방지하고 있습니다. 이런 경영진의 관심을 통해 보안 수준 향상에 즉각적인 효과를 나타나도록 하며 보안 투자 및 인력 채용 확대로 이어지는 선순환 구조를 만들 수 있었습니다.

② 당사의 정보보호 체계의 근간인 ISO27001의 신규 규격인 2022버전으로 전환심사를 수행하여 관리체계 및 정책을 최신화 하였습니다. 이를 토대로 ‘25년 계획된 지방사업장 현장 보안점검을 수행하여

발견된 미흡사항에 대해 100% 개선조치를 완료하였습니다. 또한 총 15개 해외법인에 대해서 출장을 통한 현장점검 및 수준진단을 실시하고 권역별 담당자를 통한 개선조치를 진행하여 공급망 전반 보안수준을 향상 시킬 수 있었습니다. 이에 더하여 해외법인의 경우 본사 지원을 통한 필수 보안솔루션 구축, 소스코드 점검, 웹취약점 점검, 인프라 취약점 점검과 같은 보안성 검토 절차를 확립하였습니다. 전사 모든 시스템에 대해 화이트 해커를 통한 공격자 시뮬레이션 점검을 통해 추가적인 침투 경로를 식별하여 조치하고, 사이버 모의훈련을 통해 프로세스를 점검함으로써 사이버 위협에 대한 사전 예방 체계를 구축하고 있습니다.

③ 정보보안 포털 시스템 “지키미”를 구축 완료하여 정보자산 관리, 예외처리 신청/승인, 보안 KPI 관리 등 관리적인 뿐만 아니라 이용자 측면의 효율성을 크게 향상시켜 임직원의 큰 만족도를 확인할 수 있었습니다. 당사는 Splunk 솔루션을 통한 빅데이터 분석 기반 정보 유출 모니터링을 상시 수행하고 있으며 추가적으로 네트워크 단의 모든 패킷을 분석하는 NDLP 솔루션을 금년 구축 완료하여 생성형 AI를 통한 정보 유출 차단, 메일 및 첨부파일 상세 분석, 이미지 내 Text 추출 등이 가능하도록 모니터링 수준을 한층 강화하였습니다. 또한 영업비밀 보호를 위한 연 1회 서약서 징구, 보안인식제고 교육/개인정보 보호 교육 수행, 분기별 피싱메일 모의훈련을 수행하고 그 결과를 보안KPI와 연동하여 수행 효과성을 높임으로써 정보유출 모니터링 및 보안인식 제고를 병행하고 있습니다.

④ 정보보호 공시 의무 대상자로서 당사의 보안투자 및 인력현황에 대해 정보보호공시 포털을 통해 매년 투명하게 공개하고 있습니다. 또한 보안조직의 실급 구성, CISO 및 CPO 역할 통합을 통해 보안 전담 조직의 역할을 강화하여 보안 컨트롤타워로서의 기능을 충실히 수행할 수 있게 되었습니다. 이를 통해 오토비즈, 채용 등 개인정보 수탁사 100여개에 대한 보안점검을 통해 개인정보 라이프 사이클 전반 안전성 확보조치를 이행하고 있습니다. 추가적으로 PC 內 개인정보를 검출하는 솔루션을 도입하여 개인정보를 검출하고 암호화 및 삭제하도록 정기적인 캠페인을 운영하고 있습니다. 특히 올해 크고 굵직한 보안 사고들로 인해 과학기술정보통신부의 다양한 긴급 보안점검 요청으로 IT자산 실사, 인터넷 접점 자산 관리, 취약점 및 백업체계 점검 등 수행하여 관리 체계 전반에 대해 다시 한번 점검해 볼 수 있는 계기가 되었습니다.

⑤ 최신 보안위협 트렌드 중 하나가 협력사를 통한 침투 및 보안사고 발생이었습니다. 물류, 유통, 해운 사업 전반 협력사에 대해 중요도 평가를 수행하였으며, 중요 협력사에 대한 보안 수준 점검 및 가이드를 제공하고 있습니다. 이를 토대로 네트워크 망분리를 통한 불필요한 침투 경로를 사전 차단한 부분은 상당히 의미있는 성과였습니다. 협력사 대상 보안 세미나를 개최하여 역량 향상 프로그램을 제공하고 우수 협력사에 대해 포상도 수행함으로써 Supply Chain 전반에 대해 실질적인 보안수준 향상을 위한 활동을 지속 해나가고 있습니다.

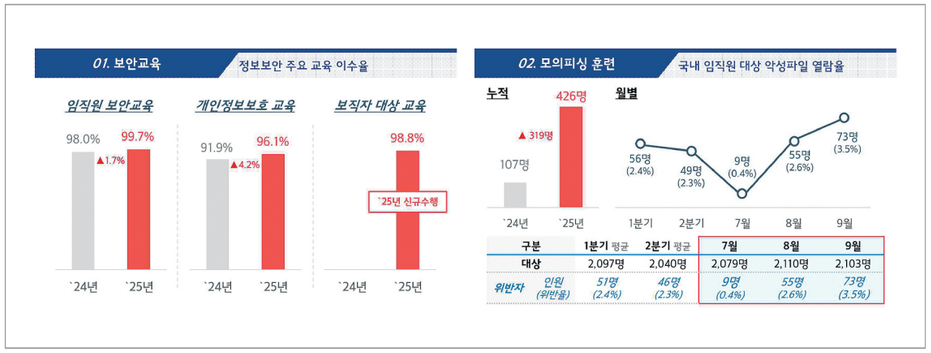
추진 성과

현대글로비스가 수립한 정보보호 전략과 로드맵에 따른 중점 추진 과제들은 정량적·정석적 측면에서 모두 괄목할 성과를 거두었습니다. 보안사고는 ’0건‘을 지속 유지하고 있으며 임직원 보안교육 및 개인정보보호 교육 이수율은 100%에 가깝게 향상되었습니다. 모의피싱 훈련 솔루션 고도화를 통해 실전과 유사한 훈련을 수행하여 임직원의 경각심을 고취시킬 수 있는 계기가 되었습니다.

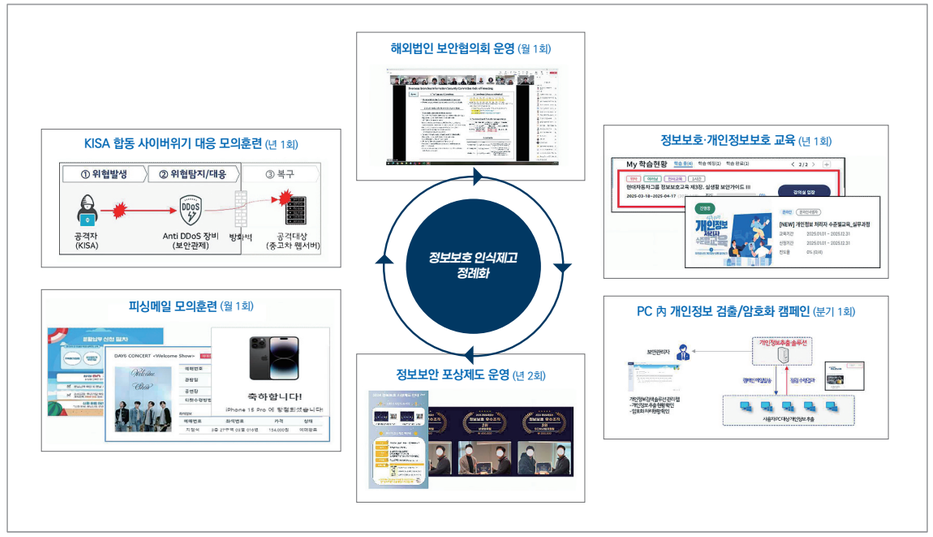
경영진의 정보보호 이해도와 조직 내 신뢰도도 향상되어, 전사 정보보호 예산은 전년 대비 46% 증액되었습니다. 신규 보안솔루션 구축, 보안성 검토 절차 확산전개를 통해 정보유출 모니터링 및 사이버 침해예방에 있어 더욱 세밀한 대응이 가능하게 되었습니다.

보안KPI 운영, 부서 정보보안 담당자 지정, 정기 협의회 수행으로 보안 운영 및 협업 체계를 갖추었습니다. 해외법인, 지방사업장, 협력사에 대한 현장 보안 점검 활동 강화, 정기 협의체 수행, 보안 세미나 개최, 포상 제도 도입을 통한 인식제고 활동으로 정보보안 거버넌스 체계의 내실을 더욱 견고히 다질 수 있었습니다.

〈교육 이수율 및 모의피싱 훈련 위반자 변화 그래프〉



〈주요 정보보호 인식 제고 활동〉



향후 계획 및 기대성과

향후에는 정보보안 투자를 더욱 확대하여 퍼블릭 클라우드 보안체계를 구축하여 퍼블릭 클라우드 보안솔루션에 대한 가시성 및 거버넌스를 확보할 예정입니다.

추가적으로 AI 위협에 대한 모니터링은 고도화하여 지속 수행하되 기존 사용 중인 기업용 생성형 AI뿐만 아니라 그룹 자체개발 생성형 AI 활용을 통하여 안전한 업무환경과 임직원 업무 효율성을 동시에 지원할 예정입니다.

또한 B2C 영역에 대한 ISMS-P 인증을 선제적으로 취득하여 정보보호체계를 더욱 고도화하고 대외 정보보안 신뢰도를 한층 향상시킬 수 있을 것으로 기대합니다. Global Top Tier SCM 전문 기업으로서 보안 분야에서도 모범적인 혁신 및 벤치마킹 롤 모델을 지속 제공하는 기업으로 유지될 수 있도록 하겠습니다.

CISO 인터뷰

Interview

한승연 CISO는
"보안은 선택이 아닌 전략이다 -
당사는 임직원의 보안 인식을 높이고
급변하는 환경에 맞춰 보안 패러다임을
전환함으로써 위협에 기민하게 대응할 수
있는 체계를 강화하고 있습니다.
이를 통해 최고 수준의 지속 가능한 보안
환경을 구축하여 비즈니스 연속성과 비전
달성을 지원하는 것이 핵심 목표입니다."
라고 전했습니다.

고려아연

고려아연 주식회사

비철금속 제련소 현장 제어시스템의 OT 보안 체계 구축 사례

기업 개요

설립연도	1974년
주요사업	종합 비철금속 제련업
임직원 수	1,909명
정보보호 조직	정보보호부문(10명, CISO 포함)
정보보호 예산	30억원(2024년 기준)
기업 특성	고려아연은 비철금속을 생산하는 업체로, 생산망 현장 제어시스템의 가용성이 매우 중요한 만큼 OT 시스템 보안이 핵심 과제입니다.

추진 배경

고려아연은 비철금속 분야 세계 1위 생산업체로, 울산 온산공단 제련소에서 아연, 연, 동, 금, 은 등 다양한 비철금속을 생산하고 있습니다. 특히 전 세계 아연 생산량의 8.4%를 차지하며, 단일 제련소 기준 세계 최대 규모를 자랑합니다.

제조업 특성상 보안 사고나 시스템 오류는 생산 일정 지연, 품질 저하 등 심각한 리스크로 이어지며, 이는 곧 생산 효율 저하와 이익 감소로 직결됩니다.

당사는 2019년 10월 “크립토락커(CryptoLocker)” 랜섬웨어 공격으로 업무망 시스템 437대의 파일이 암호화되는 사고를 겪었습니다. 이로 인해 일부 업무가 마비되었고, 복구까지 약 1개월이 소요되었습니다. 이 사건은 전사적 보안 강화의 필요성을 절실히 깨닫는 계기가 되었습니다.

당시 업무망과 제어망 사이에 연결 구간은 있었지만, 방화벽이 설치되어 피해가 제어망으로 확산되지 않았습니다. 만약 제어시스템까지 감염되었다면 피해 규모는 상상할 수 없을 정도로 컸을 것입니다.

이후 당사는 업무망뿐 아니라 제조 현장 보안 강화를 위한 프로젝트를 추진했습니다. 프로젝트 착수 전 점검 결과, 수많은 OT 자산이 운영되고 있음에도 체계적인 자산 리스트가 없었고, 시스템 관리가 벤더사에 의존되어 기본적인 백신조차 적용되지 않은 상태였습니다.

또한 현장 근무자의 낮은 보안 인식으로 인해 악성코드 감염 USB 사용, 외부 협력업체 개인 노트북 연결 등이 빈번하게 발생했고, 그로 인해 공장별 간헐적인 악성코드 감염 문제가 지속되었습니다.

이러한 리스크를 줄이기 위해 당사는 과학기술정보통신부와 한국인터넷진흥원이 발간한 ‘스마트공장 보안모델 해설서’를 참고하여 OT 보안 강화 프로젝트를 본격 추진했습니다. 운영 중인 모든 자산을 체계적으로 관리하기 위해 전 공장 자산 실사 및 리스트 정비, 공장 보안 정책 수립, OT 보안 솔루션 적용 등 다양한 조치를 시행했으며, 현재도 지속적인 개선을 이어가고 있습니다.

추진 내용 및 추진 경과

고려아연은 현장 시스템 보안을 강화하기 위해 기초 단계부터 솔루션 구축까지 다양한 조치를 단계적으로 시행했습니다.

① 내부 보안 위협 차단

현장 제어시스템은 외부 인터넷과 단절된 폐쇄망(Air-Gap) 환경에서 운영되어 외부 공격 가능성은 낮지만, 개인용 USB 사용과 유지보수 엔지니어 노트북 연결 등 내부 위협이 존재했습니다. 이를 해결하기 위해 PLC, DCS, HMI PC, 네트워크 장치의 LAN 및 USB 포트에 포트락 장치를 설치하여 불필요한 기기 연결을 차단했습니다. 또한 업무망과 제어망 접점 구간에 단방향 솔루션을 구축해 외부 네트워크와의 역방향 통신을 원천 차단, 중요 제어시스템의 무결성을 확보했습니다.

② 보안 전략 및 마스터 플랜 수립

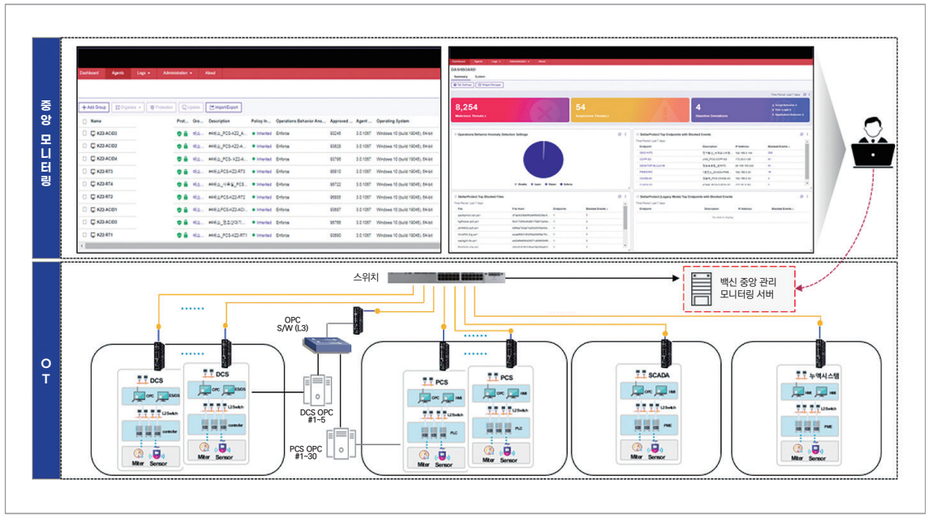
전문가 컨설팅을 통해 현장 시스템의 보안 현황을 점검하고 취약점을 식별했습니다. OT 보안 위협 분석, 산업 보안 트렌드 파악, Best Practice 검토를 통해 단기 대응 방안과 장기 개선 계획을 포함한 마스터 플랜을 마련했습니다.

구분	내용
단기 목표	즉각적 위험 요소 제거, 보안솔루션 도입, 중앙 모니터링 체계 구축, 신규 자산 도입 프로세스 개선
장기 목표	보안 정책 강화, 근무자 보안 교육, EOS 시스템 업그레이드 등 지속적 보안 수준 향상

③ OT 전용 보안솔루션 도입

현장 시스템 특성상 가용성이 중요하고, 장기간 동일 환경을 유지하기 때문에 강력한 보안 설정이 필수입니다. 이에 따라 화이트리스트 기반 실행 제어, 백신 기능, 매체 제어 기능을 포함한 단일 에이전트를 설치했습니다. 화이트리스트에 없는 프로그램은 실행을 차단하여 시스템 안정성을 확보했습니다. 또한, 제어시스템 로그를 중앙에서 모니터링할 수 있도록 네트워크를 Segmentation 단위로 구분, 각 영역별 방화벽을 설치하고 특정 프로토콜·포트만 허용하는 정책을 적용했습니다. 이를 통해 실시간 로그 감시 및 분석이 가능해져 보안 가시성을 크게 강화했습니다.

〈OT 제어시스템 보안 모니터링 체계 구축〉



④ 이상징후 탐지 솔루션 도입

현장 네트워크 및 제어시스템에서 발생하는 비정상 트래픽, 이상 행위, 잠재적 침입 시도를 탐지하기 위해 OT 환경 특화 솔루션인 포터블 이상 징후 탐지 솔루션을 도입했습니다. 해당 솔루션을 통해 네트워크 분석과 머신러닝 기반 이상징후 탐지를 통해 내부 위협, 네트워크 구성 점검, 설정 오류 등을 식별하고 가시화하였으며, 이를 통해 기존 보안 체계에서 놓칠 수 있는 운영 리스크를 선제적으로 대응할 수 있는 기반을 마련하였습니다.

⑤ 제어시스템 로컬 백업 솔루션 도입

제어시스템은 제조 현장에서 가장 우선순위가 높은 핵심 시스템으로, 상시 가용성을 확보하고 사고 발생 시 신속한 복구가 무엇보다 중요합니다. 이를 위해 각 현장 제어시스템에 로컬 백업 솔루션을 적용하여 설정 파일, 운영 데이터, 시스템 이미지를 주기적으로 백업하고, 장애 발생 시 즉시 복원할 수 있는 체계를 구축했습니다.

솔루션 도입을 통해 다운타임을 최소화하고 생산 연속성을 확보했으며, 랜섬웨어 등 치명적 사고 발생 시 피해를 크게 줄일 수 있는 기반을 마련했습니다.

⑥ 임직원 보안인식 제고 교육

기술적 조치와 함께 인적 보안 리스크를 줄이기 위해, 임직원 및 협력업체 직원을 대상으로 정기적인

보안 교육과 훈련을 실시했습니다. 악성 메일 대응 훈련, 보안 관련 중요 문구 노출, 보안 홍보물 배포 등 다양한 활동을 통해 현장 근무자의 보안 인식을 강화했습니다.

이러한 조치를 통해 USB 사용이나 비인가 장치 연결 등 인적 요인으로 인한 보안 사고를 예방하고, 전사적인 보안 문화 정착을 위한 기반을 마련했습니다.

〈임직원 정보보호 인식 제고 교육 진행〉

추진 성과

고려아연은 단계적인 보안 강화 조치를 통해 현장 제어시스템의 보안 수준을 획기적으로 향상시켰습니다. 우선 포트락을 설치하여 USB 및 비인가 장치의 연결을 원천 차단하고, 업무망과 제어망 간 단방향 솔루션을 적용하여 역방향 통신을 차단함으로써 내부 위협으로 인한 악성코드 유입 경로를 제거하고 제어시스템의 무결성을 확보했습니다.

또한 전문가 컨설팅을 통해 주요 취약점을 식별하고, 단기 및 장기 개선 목표를 포함한 마스터 플랜을 수립하여 보안 정책을 표준화했습니다. 이를 기반으로 신규 자산 도입 시 보안 검토 절차를 체계적으로 적용할 수 있는 구조도 마련했습니다. 아울러 OT 전용 보안 솔루션을 도입하여 화이트리스트 기반 실행 제어, 백신 기능, 매체 제어 기능을 적용하고, 중앙 모니터링 체계를 구축해 실시간 로그 분석과 이상 행위 탐지가 가능하도록 개선했습니다.

더불어 이상징후 탐지 솔루션을 적용해 비정상 트래픽과 잠재적 침입 시도를 실시간으로 탐지하고, 머신러닝 기반 분석을 통해 제로데이 공격과 설정 오류를 조기에 식별함으로써 운영 리스크에 선제적으로 대응할 수 있는 기반을 마련했습니다. 또한 제어시스템 로컬 백업 솔루션을 통해 설정 파일과 운영 데이터를 주기적으로 백업하고, 장애 발생 시 즉시 복원할 수 있는 체계를 구축하여 다운타임을 최소화하고 생산 연속성을 확보했습니다.

이와 같은 보안 강화 조치의 결과, 현장 시스템 보안 사고 발생률은 2025년 0건을 달성했으며, 주요 현장 시스템의 보안 현황을 중앙에서 모니터링함으로써 이벤트 대응 시간을 평균 90% 단축하는 성과를 거두었습니다. 또한 정기 교육과 보안 홍보 활동을 통해 현장 근무자의 보안 인식을 높임으로써, 전사적인 보안 문화 정착을 위한 기반을 마련했습니다.

향후계획 및 기대성과

2022년부터 추진해 온 OT 보안 강화 프로젝트를 통해 기본적인 보안 관리 체계를 구축했으나, 여전히 보완해야 할 부분이 많이 남아 있는 것이 사실입니다. “보안에 지나침은 없다”는 말처럼, 당사는 현장 제어시스템의 보안 수준을 지속적으로 강화하기 위해 다음과 같은 프로젝트를 계획하고 있습니다.

우선, OT 전용 SIEM 시스템 구축을 통해 상관분석 기반의 모니터링 체계를 고도화할 예정입니다. 이를 통해 다양한 OT 보안 솔루션 로그를 통합 수집하고 이벤트 간 연관성을 분석함으로써, 보다 정확하고 정교한 위협 탐지가 가능해질 것으로 기대합니다. 또한 경고 발생 시 즉각적으로 대응할 수 있도록 실시간 알림 및 대응 프로세스를 정교화하여 초기 대응 능력 역시 대폭 강화할 계획입니다. 이러한 체계 구축을 통해 단편적으로 발생하던 보안 이벤트를 통합적으로 분석하고, OT 환경 전반에 대한 위협 가시성을 한층 높일 수 있을 것입니다.

아울러, 현장 근무자 대상 보안 교육 체계를 지속적으로 강화하여 인적 보안 사고를 예방하고 보안 인식을 전사적으로 제고할 계획입니다. 실제 상황을 기반으로 한 시나리오형 해킹 모의훈련을 확대하고, 현장 근무자를 대상으로 정기적인 OT 보안 교육과 사고 사례 공유를 추진하여 실질적인 대응 역량을 향상시킬 예정입니다. 이를 통해 전사적인 OT 보안 문화를 보다 굳건히 정착시키고, 현장에서 자발적인 보안 실천이 이루어지는 환경을 구축해 나가고자 합니다.

CISO 인터뷰

Interview

황인구 CISO는 제조업 기업을 대상으로 한 해킹 공격이 지속적으로 증가하고 있으며, 이로 인해 생산에 차질이 발생할 경우 기업 가치와 대외 신뢰도에 심각한 손상이 초래될 수 있다고 강조했습니다.

특히 OT 환경을 노린 랜섬웨어 및 공급망 공격이 늘어나는 상황에서, 사전 예방 중심의 보안 체계 강화와 함께 현장에서 운영 중인 자산의 현황을 정확히 파악하는 것이 무엇보다 중요하다고 언급했습니다.