OpenSoftLab

SECURITY OPERATION PORTAL

# LUNA™ SEC-OPS

# 통합 보안 운영 플랫폼

분산된 보안 솔루션을 통합 거버넌스로 관리하고,
반복 업무는 자동화해 관제와 대응에 집중하게 합니다.

보안포탈이 필요한 이유

# 급증하는 탐지와 보안 업무, 분절된 처리 흐름이 운영의 한계로 이어집니다.

복잡해지는 보안 환경, 파편화된 대응을 넘어 통합 보안 운영으로 나아가야 합니다.

- **알림은 콘솔에**
  장비별 화면과 이벤트 목록
- **소명은 메일에**
  담당자별 요청과 회신
- **조치는 문서에**
  사후 정리와 보고 자료
- **근거는 곳곳에**
  나중에 설명하기 어려운 이력

탐지로 끝나지 않고, 처리한 근거까지 남깁니다. LUNA SecOps는 탐지된 이벤트를 케이스·소명·조치 이력으로 이어 보안 운영의 연속성을 확보합니다.

## 탐지 이후의 처리 방식이 곧 보안 운영의 품질입니다.

같은 이벤트라도 운영 방식이 다르면 결과가 달라집니다.

| BEFORE · 장비 중심 운영 | | AFTER · 포털 중심 운영 | |
|---|---|---|---|
| 콘솔마다 따로 확인 | 분석가가 벤더별 콘솔을 일일이 열어 같은 이벤트를 중복 확인합니다. | 케이스 하나로 전환 | 탐지 데이터가 즉시 업무 단위로 묶여 처리 대상이 한 번에 정리됩니다. |
| 메일·메신저로 재촉 | 담당자 연락처를 찾아 메일·메신저·전화로 일일이 소명을 요청합니다. | 시나리오 기반 자동 매핑 | 시나리오에 따라 담당자가 자동 지정되어(수동 지정 가능) 확인 시간이 줄어듭니다. |
| 조치는 각자 메모로 | 조치 결과가 개인 문서나 수기 메모로 남아 나중엔 누구도 확신하지 못합니다. | 상태가 자동으로 누적 | 담당자·소명·조치 상태가 같은 흐름 안에서 실시간으로 남습니다. |
| 감사 때마다 재구성 | 누가 언제 무엇을 처리했는지, 감사나 사고 때마다 처음부터 다시 짜맞춰야 합니다. | 클릭 한 번으로 근거 제시 | 이벤트별 처리 이력이 이미 남아 있어 바로 꺼내 보여줄 수 있습니다. |

**핵심은 더 많은 알림이 아니라, 보안 이벤트를 설명 가능한 처리 과정으로 바꾸는 것입니다.**

OpenSoftLab

# 탐지된 이벤트를 넘어 보안운영의 전 과정을 하나의 흐름으로 완성합니다.

탐지 데이터 처리에서 케이스 생성, 소명, 조치 상태 관리까지 이어지는 보안 워크플로우

### 단일 대시보드 기반 통합 모니터링

탐지자산의 운영 극대화를 통한 신속한 의사결정과 통합가시성 제공


탐지

### 이벤트를 업무 단위로 정리

여러 장비에서 들어온 데이터를 처리 가능한 케이스로 묶고 담당 범위를 명확히 합니다.

케이스

### 소명 요청과 회신을 연결

담당자는 로그인 없이 토큰 링크로 소명을 제출하고, 그 회신은 업무 이력에 남습니다.

소명

### 조치 상태와 근거를 추적

누가 확인했고 어떤 조치로 닫혔는지 한 흐름으로 남겨 사후 확인에 활용합니다.

리포트

### 리포트 빌더로 흐름을 마무리

일간·주간·월간 등 원하는 주기로 처리 현황을 동적 보고서로 자동 생성해, 포탈의 모든 기록이 리포트 하나로 남습니다.

**LUNA SecOps는 여러 보안 시스템 데이터를 고객이 처리할 수 있는 보안포탈 업무로 바꿉니다.**

**고객사 관리자**
조직 전체가 지금 얼마나 안전한지 요약 지표로 파악

**테넌트 담당자**
내 담당 범위의 소명 처리와 조치 결과 등록

**SOC 분석가**
실제 봐야 할 이벤트를 케이스로 전환·소명 요청

**CISO·보안 책임자**
리스크 추세와 감사·컴플라이언스 대응 이력 확인

# 탐지 데이터를 업무의 언어로, 조치 이력을 운영의 자산으로

공통 데이터셋 수집부터 룰셋 매핑, 티켓·소명·신청서·시스템 연계까지 하나로 이어집니다


여러 벤더의 보안 데이터가 공통 데이터셋으로 모여 룰셋 매핑을 거쳐 티켓이 발행됩니다. 발행된 티켓은 **소명 요청으로 처리하거나, 보안정책 신청서로 이어 처리**할 수 있습니다.

**개발 공수 절감**

## 탐지 운영

공통 데이터셋 → 룰셋 매핑 → 티켓 발행 → 소명

**수집** — 공통 데이터셋
여러 벤더 로그를 한 곳으로 수집

**분석** — 룰셋 매핑
위험도별 시나리오 자동 분류

**발행** — 티켓 발행
시나리오 기반 자동 티켓 발행

**소명** — 소명 요청
시나리오 기반 자동 소명 요청

## 보안 행정

신청서 → 결재 → 정책 적용 → 시스템 연계

**신청** — 보안정책 신청서
발행된 티켓과 연계된 예외 신청서 작성

**승인** — 결재·승인
전결, 병렬 등 결재선 처리

**반영** — 정책 적용
승인과 동시에 보안 시스템에 자동 적용 요청

**연계** — 시스템 연계
설정은 자동으로, 담당자는 확인만 진행

### 특정 벤더에 묶이지 않는 폭넓은 연동

Splunk, Stellar Cyber를 포함해 다양한 보안 솔루션을 공통 데이터셋 표준으로 받아들입니다.

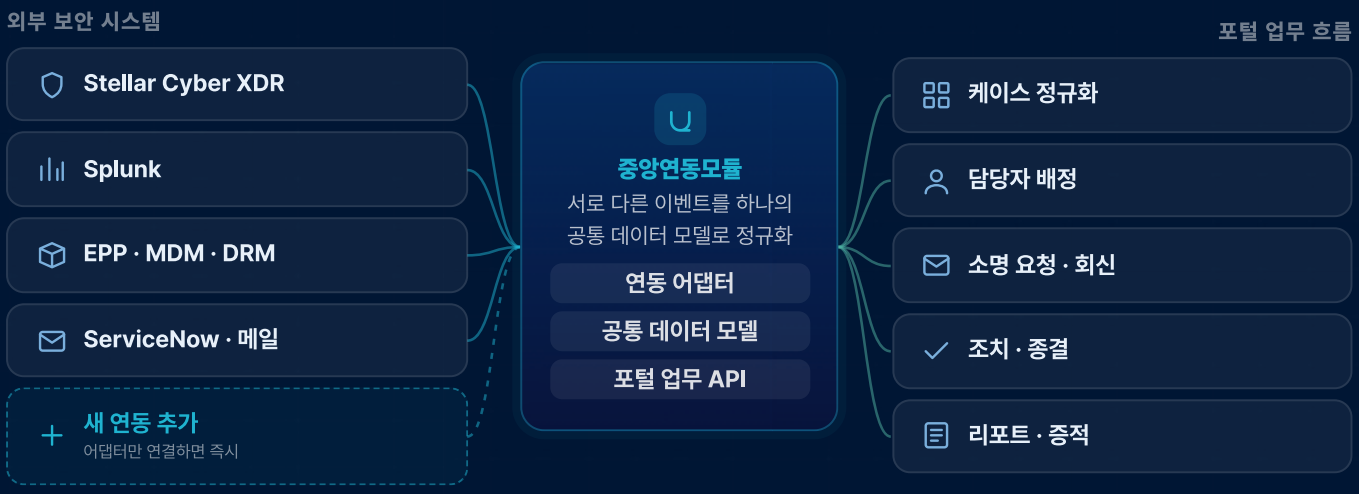
### 정책이 바뀌어도, 시스템 개발 요청이 필요 없습니다

새 요청이 생겨도 신청·승인·반영·증적이 하나의 화면 흐름 안에서 끝납니다.

**정책이 바뀌어도, 담당자가 할 일은 신청서 하나뿐입니다.**

# 보안 시스템이 늘어나도, 연결만 하면 끝

서로 다른 보안 시스템을 공통 데이터 모델로 정규화 — 새 시스템이 들어와도 어댑터만 연결하면 포털의 확인·소명·조치 흐름은 그대로입니다.




### 새 장비를 붙여도 고객의 운영 화면은 바뀌지 않습니다.

보안 시스템별 알림 형식과 API 차이는 중앙연동모듈에서 흡수하고, 고객은 익숙한 포털 흐름 안에서 사건을 확인하고 처리합니다.

### 도입 포인트는 연결보다 운영 표준화입니다.

각종 보안 시스템 데이터를 고객별 보안포탈 흐름으로 통합 관리합니다.

연동

### 보안 시스템 연동을 표준화

Stellar Cyber, Splunk 같은 XDR/SIEM부터 엔드포인트·DRM·ITSM까지 같은 흐름으로 연결합니다.

정규화

### 서로 다른 이벤트 로그를 하나의 형식으로

보안 시스템마다 다른 이벤트·알림 형식을 공통 데이터 모델로 변환해 포털 업무 API로 전달합니다.

분리

### 고객·테넌트별 데이터와 권한 분리

고객사별 데이터와 담당 범위를 분리해, 사용자는 허용된 업무 범위 안에서만 확인하고 처리합니다.

확장

### 시스템이 늘어도 같은 운영 방식 유지

연동 대상이 늘어나도 포털의 확인·소명·조치 흐름은 그대로 유지됩니다.

### 처리 이력까지 남는 운영 체계

연동된 시스템에서 발생한 사건은 담당자 배정부터 소명 회신, 조치 결과까지 하나의 이력으로 남습니다.

중앙연동모듈 · 케이스 정규화 · 처리 이력

### 각종 시스템을 연동해도 같은 화면

XDR/SIEM부터 ITSM, 협업 도구까지 연동 대상이 늘어나도 고객은 항상 같은 보안포탈 화면에서 확인합니다.

각종 시스템 연동 · 상태 추적 · 고객별 권한

**여러 보안 시스템 위에, 하나의 보안포탈 운영 경험을 만듭니다.**

OpenSoftLab

# 보안 업무의 시작부터 끝까지, LUNA SecOps가 하나의 기준이 됩니다.

LUNA SecOps는 탐지 이후의 케이스 전환·소명 요청·조치 추적·처리 이력을 하나의 포털에서 연결합니다.

- **탐지 이후 처리가 제각각입니다**
  케이스, 담당자, 소명, 조치 상태를 같은 화면에서 이어볼 수 있어야 합니다.
- **외부 담당자 소명이 번거롭습니다**
  로그인 없이 접근 가능한 토큰 링크로 소명 회신을 받을 수 있습니다.
- **여러 보안 시스템을 함께 봐야 합니다**
  각종 시스템을 연동해 데이터를 공통 모델에 맞춰 정리합니다.

## 도입 검토 FAQ 고객이 실제로 묻는 질문

### 기존 XDR/SIEM이 있는데 왜 필요합니까?

탐지 도구를 바꾸는 제품이 아닙니다. 탐지 결과를 케이스, 소명, 조치 이력으로 이어지는 업무 흐름으로 바꿉니다.

### 외부 담당자도 소명을 제출할 수 있습니까?

가능합니다. 로그인 계정이 없어도 토큰 기반 외부 링크로 소명 내용을 작성하고 제출할 수 있습니다.

### 부서·담당자별 권한은 어떻게 분리됩니까?

담당 범위별 데이터와 화면을 분리합니다. 사용자는 허용된 업무 안에서만 현황과 요청을 확인합니다.

### 처리 결과를 나중에 추적할 수 있습니까?

가능합니다. 이벤트별 담당자, 소명 회신, 조치 상태, 처리 이력을 남겨 사후 확인과 보고에 활용할 수 있습니다.

## 보안 이벤트 처리, 이제 단일 운영 흐름으로 완성하세요.

우리 조직의 보안 이벤트가 어떤 데이터에서 시작되고, 누가 확인하며, 어떤 소명과 조치로 닫히는지 한 흐름으로 확인할 수 있습니다.


COMPANY
**(주)오픈소프트랩**

TEL
**02-6941-0501**

CONTACT
**010-9082-2179**

MAIL
**osl@opensoftlab.kr**



**주소** 서울 금천구 가산디지털1로 196, 907호 · 제품 상담 및 도입 문의는 QR 또는 osl@opensoftlab.kr로 연락해 주세요.