TIER 2 · 글로벌 보안 위협 수집 & 코드·API 이중 방어 규칙 컴파일러

2026.11 | Enterprise Edition v3.8

SyncWatch

국내외 8개 공인 보안 채널의 신규 취약점 정보를 모아 코드 점검 기준과 API 차단 규칙으로 바꿔 주는 보안 도우미

매일 발표되는 영문 보안 권고(CVE)와 KISA 공지를 자동으로 수집·정리하여,
개발팀용 취약 패키지 점검 기준과 운영팀용 API 차단 규칙 초안을 빠르게 준비합니다.

핵심 제공 가치

국내외 8대 보안 채널 24시간 수집

KISA 보호나라, 미국 CISA, NVD, GitHub 등 공인 위협 정보를 실시간 자동 입수

읽기만 하는 공지를 '실행 규칙'으로 변환

줄글로 된 보안 권고문을 코드 취약점 검사식과 API 방화벽 차단식으로 자동 컴파일

코드 점검 + API 방어 이중(Dual) 공급

SyncVerse(소스코드 패치용)와 SyncAPIM(실시간 트래픽 차단용)에 동시 배포

공격·정상 샘플 샌드박스 사전 검증

만들어진 방어 규칙이 정상 요청을 잘못 막지 않는지 자체 샌드박스에서 사전 시험

발행처 : 주식회사 엠파시 (Empasy Inc.) | 문의 : biz@empasy.io
문서 포털 : https://doc.empasy.com | 라이브 데모 : https://sync.empasy.io

SYNCWATCH CORE CAPABILITIES

핵심 구성 요약

01 8대 공인 보안 피드 자동 수집 & 5단계 안전 검증

OSV.dev, GitHub GHSA, NIST NVD, CISA KEV, Nuclei, OWASP CRS, MITRE ATLAS(AI 위협), KISA 보호나라를 안전하게 상시 수집합니다.

02 보안 권고 정규화 & 사내 자산 영향도 매칭

제각각인 국내외 보안 공지 포맷을 단일 표준 원장(CVSS 위험도·악용 여부·영향 언어)으로 통합하고 사내 소프트웨어 자산과 대조합니다.

03 개발팀용 '취약 패키지·코드 점검 규칙' 추출 (SyncVerse용)

보안 권고문에서 위험한 라이브러리 버전 범위, 패치 버전, 취약 함수명, SAST 코드 정규식과 조치 가이드를 자동으로 뽑아냅니다.

04 운영팀용 '공격 차단 시그니처' 컴파일 (SyncAPIM용)

해킹 패킷의 특징을 분해하여 HTTP 검사 위치(URI/헤더/바디)와 방어 조건식(SpEL)을 만들고, 정·오탐 샘플 테스트 통과 후 배포합니다.

취약점 공지 확인부터 실제 방어 규칙 적용까지의 시차를 크게 줄입니다

해커는 보안 취약점(CVE)이 공개된 지 몇 시간 만에 자동화된 공격을 시작하지만, 기업은 사람이 공지를 읽고 방화벽 룰을 짜느라 며칠씩 늦는 구조적 한계를 해결합니다.

현재 현장에서 겪는 어려움 (AS-IS)

01. 매일 쏟아지는 수백 건의 영문 보안 공지를 사람이 다 못 읽음

NVD, GitHub, KISA 등 여러 사이트에 올라오는 수많은 취약점 공지 중 우리 회사 시스템(Java/Spring, Vue, Docker 등)과 관련된 것을 골라내기도 벅찹니다.

02. 보안 권고문은 '줄글 설명'이라 바로 방어 시스템에 넣을 수 없음

공지문에는 취약점 원리만 적혀 있을 뿐, 이를 실제 웹방화벽 차단 규칙이나 소스코드 점검 규칙으로 바꾸려면 보안 전문가가 수작업으로 코딩해야 합니다.

03. 운영팀(방화벽 차단)과 개발팀(소스코드 패치)의 대응이 따로 놂

보안팀이 엑셀로 취약점 목록을 정리해 개발팀에 메일로 보내면, 어느 프로젝트가 실제로 해당 라이브러리를 쓰는지 파악하고 패치하는 데 수주가 걸립니다.

04. 급하게 만든 차단 규칙이 정상 서비스를 막거나 서버를 느리게 함

충분한 검증 없이 급조한 정규식 차단 룰을 올렸다가 정규식 무한 루프(ReDoS)가 걸리거나 정상 고객 요청이 차단되는 2차 사고가 발생합니다.

SyncWatch가 풀어내는 방식 (TO-BE)

01. 8대 글로벌·국내 공인 보안 채널 자동 수집 및 한글 표준화

8대 공인 채널 연동

KISA 보호나라부터 미국 CISA 실제 악용 취약점(KEV), AI 전용 위협(MITRE ATLAS)까지 자동 수집해 위험도와 영향 기술 스택별로 깔끔하게 정리합니다.

02. 줄글 보안 공지를 '즉시 실행 가능한 2종 방어 규칙'으로 자동 변환

수작업 룰 작성 0분

보안 권고문을 분해하여 ① 소스코드/라이브러리 점검 기준(VerseAuditPack)과 ② 네트워크 공격 차단 규칙(ApimDefensePack)으로 자동 컴파일합니다.

03. SyncAPIM(즉시 공격 차단) + SyncVerse(근본 코드 패치) 동시 공급

대응 시간 수일 -> 1분

버튼 하나로 운영 게이트웨이에는 실시간 가상 패치를 내려보내고, 개발 관제탑에는 취약 라이브러리 업그레이드 가이드를 동시에 전달합니다.

04. 샌드박스 정탐/오탐 테스트 및 ReDoS 안전성 검증 통과분만 배포

샘플 사전 시험 통과

자동 생성된 모든 규칙에 대해 공격 샘플(반드시 차단)과 정상 샘플(반드시 통과)을 대입해 공격 탐지와 정상 통과 시험을 거친 안전한 규칙만 내보냅니다.

핵심 정리 SyncWatch는 외부 보안 뉴스를 단순히 모아 보여주는 게시판이 아니라, 위협 정보를 즉시 작동하는 방어 무기로 깎아주는 '자율 보안 룰 공장'입니다.

수집 · 정규화 · 이중 방어 규칙 변환 · 샌드박스 시험 흐름

외부 인터넷에서 보안 피드를 가져올 때조차 5단계 SSRF 보안 가드를 거쳐 안전하게 수집하며, 검증된 규칙만 사내 시스템에 공급합니다.

SyncWatch 4단계 처리 흐름 (요청 접수부터 사전 확인 · 실행 · 복원 준비까지)

STEP 01 · 위협 수집

8대 보안 피드 안전 수집

5단계 SSRF 가드(사설망 차단·용량 제한)를 거쳐 국내외 8대 공인 보안 채널을 수집합니다.

STEP 02 · 정규화·분류

단일 원장 정규화 & 분류

제각각인 공지 포맷을 위험도(CVSS), 실제 악용 여부(KEV), 기술 생태계별로 표준화합니다.

확인 게이트 · 샌드박스 정·오탐 검증

ReDoS 복잡도 검사 · 공격 샘플 탐지 · 정상 요청 통과 시험 필수

STEP 03 · 듀얼 컴파일

이중(Dual) 방어 규칙 컴파일

개발팀용 '취약 패키지·코드 기준'과 운영팀용 'API 차단 시그니처' 두 가지로 자동 변환합니다.

STEP 04 · 배포·추적

전사 브로드캐스트 & 피드백

SyncVerse와 SyncAPIM에 규칙을 배포하고 실제 패치·차단 적용 완료 여부를 역추적합니다.

역할 분담 : AI가 맡는 부분과 담당자가 직접 결정하는 부분

AI 위협 컴파일러 자동 수행 영역

수집 · 정규화 · 듀얼 규칙 합성 · 검증

- 8대 글로벌·국내 보안 피드 주기적 자동 수집 및 중복 제거
- 영문 기술 권고문에서 취약 버전 범위, 패치 버전, 취약 심볼 자동 추출
- 네트워크 공격 벡터를 분해해 HTTP 위치별 정규식 및 SpEL 방어식 합성
- 양성(공격)·음성(정상) 샘플 기반 샌드박스 자동 백테스팅 수행

사람(보안 관리자) 결정 영역

수집 채널 관리 및 긴급 규칙 배포 승인

- 수집 채널별 동기화 주기 설정 및 수동 보안 공지(STIX/SARIF) 업로드
- 우리 회사 핵심 기술 스택(Maven, NPM, Docker 등) 중점 감시 필터링
- 샌드박스 검증을 통과한 신규 방어 규칙의 전사 배포 승인
- 하위 시스템(SyncVerse, SyncAPIM)의 조치 완료 피드백 현황 점검

시스템 안전 장치 영역

안전한 인바운드 수집 및 무결성 추적

- 5단계 SSRF 가드(DNS Pinning, 내부망 IP 차단, 타임아웃)로 수집 서버 보호
- 정규식 서비스 거부(ReDoS) 유발 위험 패턴 컴파일 단계에서 사전 제외
- 수집부터 파싱·컴파일·검증·배포까지 5단계 실행 로그 전수 기록
- SyncCrawl과 연동해 동적 렌더링이 필요한 국내 보안 공지까지 무결성 수집

작동 원리 | 보안 권고문이 발표된 순간부터 사내 게이트웨이와 코드 감사기에 방어 규칙이 장전되기까지 사람의 수작업 병목을 완전히 제거합니다.

8개 공인 채널 위협 유입 현황과 방어 규칙 전환 실시간 관제

활용 시점 : 오늘 새로 발표된 긴급 보안 취약점(Critical/KEV)이 몇 건인지, 그중 몇 건이 코드 점검 규칙과 API 차단 규칙으로 변환·배포되었는지 확인할 때 사용합니다.

주요 제공 기능

8대 공인 채널 실시간 관제

01 8대 수집 채널 가동 상태 및 실시간 위협 유입 지표

OSV, GHSA, NVD, CISA KEV, Nuclei, OWASP, MITRE ATLAS, KISA 8개 채널의 정상 수집 여부와 누적 보안 권고 건수를 한눈에 파악합니다.

02 심각도별(Critical/High) 및 실제 해킹 악용(KEV) 취약점 하이라이트

단순 이론적 취약점이 아니라 현재 실제 해커들이 악용 중인 긴급 위협(CISA KEV / 공개 PoC 존재)을 최상단 경보로 우선 표시합니다.

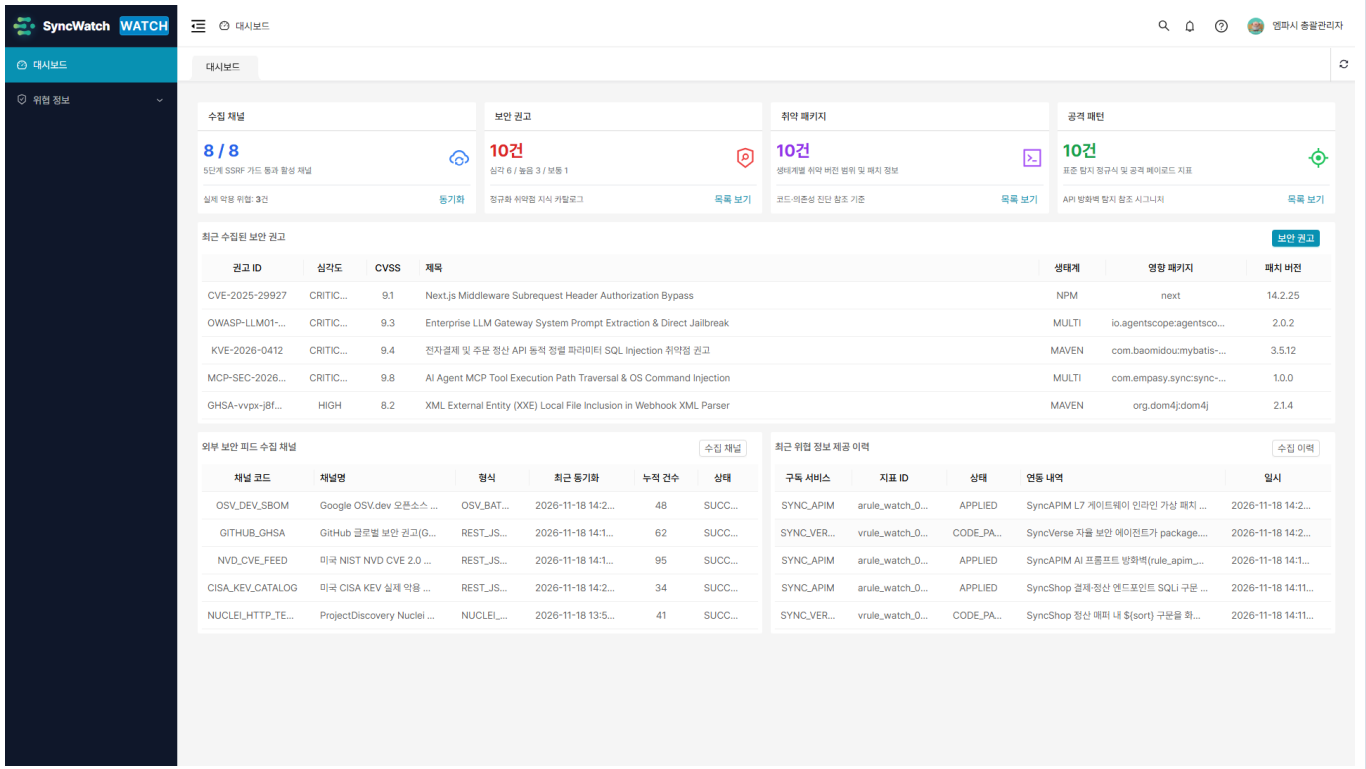
03 듀얼 아티팩트(SyncVerse 코드 규칙 / SyncAPIM 차단 규칙) 컴파일 현황

수집된 권고문으로부터 추출된 취약 패키지 점검 규칙 수와 샌드박스 검증을 통과한 API 방어 시그니처 수를 실시간으로 보여줍니다.

04 하위 서비스 배포 및 조치 완료율 실시간 추적

배포된 방어 규칙이 SyncAPIM 게이트웨이와 SyncVerse 코드 감사에 실제로 반영 완료(ACK)되었는지 상태 배지로 확인합니다.

https://sync.empasy.io/watch/dashboard



구동 화면 | SyncWatch 통합 관제 대시보드 — 8대 위협 피드 수집 현황, KEV 긴급 경보 및 듀얼 방어 규칙 컴파일 지표 (시연 데이터 기준)

실무 활용 여러 보안 사이트를 돌아다닐 필요 없이 SyncWatch 대시보드 하나로 국내외 최신 취약점과 사내 방어 태세를 동시에 점검합니다.

보안 피드 채널 관리 및 5단계 외부 연결 안전 검사

활용 시점 : 각 보안 피드 채널의 수집 주기를 조정하거나, 외부 연결이 안전한지 5단계 보안 진단 테스트를 실행하고 즉시 동기화할 때 사용합니다.

주요 제공 기능

5단계 SSRF 안전 수집

01 8대 표준 커넥터 및 KISA 보호나라(SyncCrawl 연동) 통합 관리

REST JSON, OSV Batch, RSS/Atom XML, Nuclei YAML, STIX 2.1 등 서로 다른 프로토콜의 8대 보안 피드를 단일 화면에서 제어합니다.

02 원클릭 5단계 SSRF 안전 연결 진단

외부 피드 주소 호출 전 ① URL 구문 -> ② DNS Pinning -> ③ 사설망/클라우드 메타데이터 IP 차단 -> ④ TLS 검증 -> ⑤ 응답 크기 제한을 실시간 진단합니다.

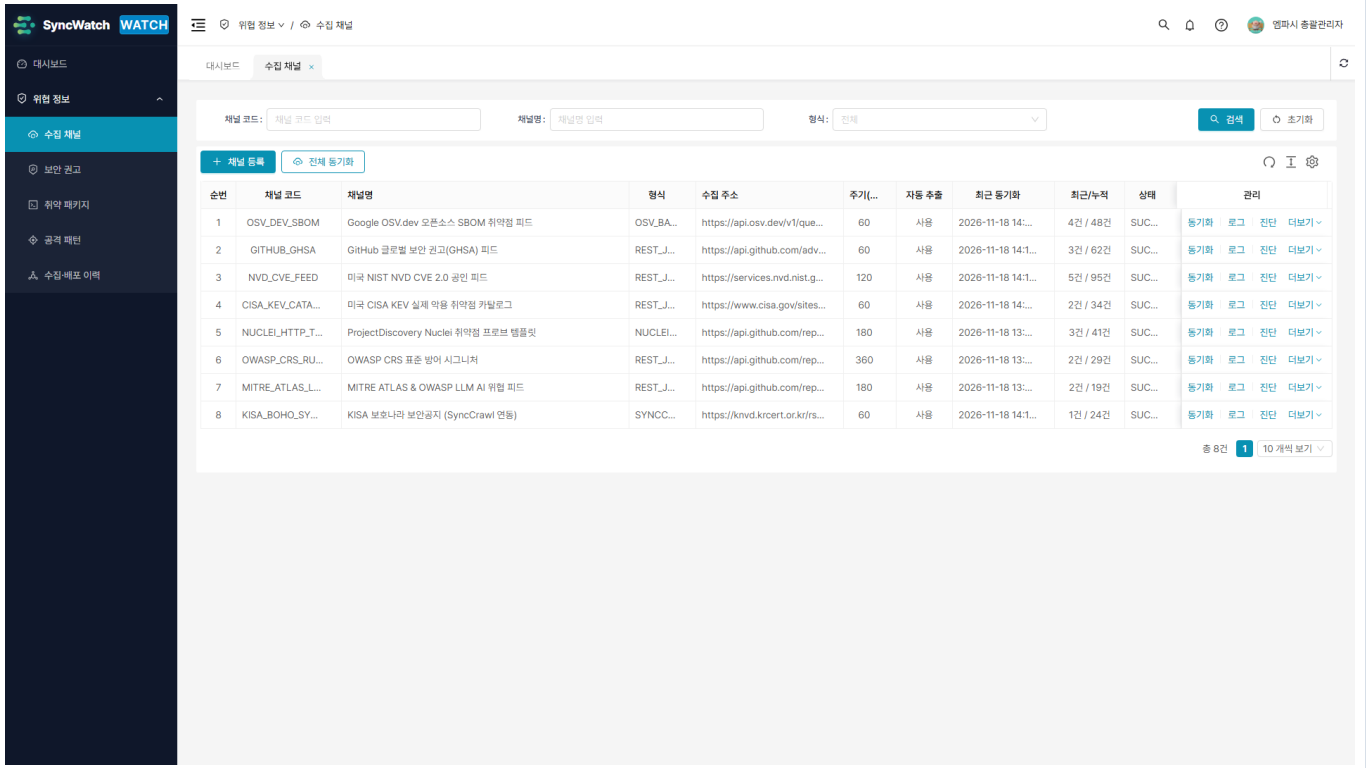
03 채널별 즉시 동기화 실행 및 수집 건수·소요 시간 확인

긴급 취약점 뉴스가 나왔을 때 정기 스케줄을 기다리지 않고 [즉시 수집] 버튼 하나로 10초 내에 최신 권고문을 가져옵니다.

04 폐쇄망 환경을 위한 STIX 2.1 / SARIF 2.1.0 오프라인 번들 반입

외부 인터넷이 완전히 차단된 망분리 환경에서는 공인 보안 번들 파일을 업로드하여 동일하게 정규화와 듀얼 룰 컴파일을 수행합니다.

https://sync.empasy.io/watch/feeds



구동 화면 | SyncWatch 보안 피드 채널 관리 — 8대 공인 채널 상태, 5단계 SSRF 연결 진단 및 즉시 동기화 (시연 데이터 기준)

실무 활용 외부 위협 정보를 가져오는 통로 자체의 보안성까지 5단계 SSRF 가드로 철저히 검증하여 안전한 수집만 허용합니다.

개발팀용 취약 오픈소스 라이브러리 및 코드 점검 기준 추출

활용 시점 : 개발팀이 사용하는 오픈소스 라이브러리 중 취약한 버전이 무엇이고 몇 버전으로 올려야 하는지, 코드 안에서 어떤 함수를 고쳐야 하는지 볼 때 사용합니다.

주요 제공 기능

개발팀 패치 가이드 자동화

01 생태계별(Maven · NPM · Go · Python · Docker) 취약 버전 및 패치 버전 명시

예: 'Spring Framework 6.1.0~6.1.13 취약 -> 6.1.14 이상으로 업그레이드'처럼 개발자가 즉시 pom.xml이나 package.json을 고칠 수 있게 안내합니다.

02 취약 함수 심볼(Affected Symbols) 및 SAST 코드 점검 정규식 제공

단순히 라이브러리 이름만 알려주는 것이 아니라 실제 문제가 되는 클래스·메소드 이름과 소스코드 정적 분석(SAST) 탐지 패턴을 함께 추출합니다.

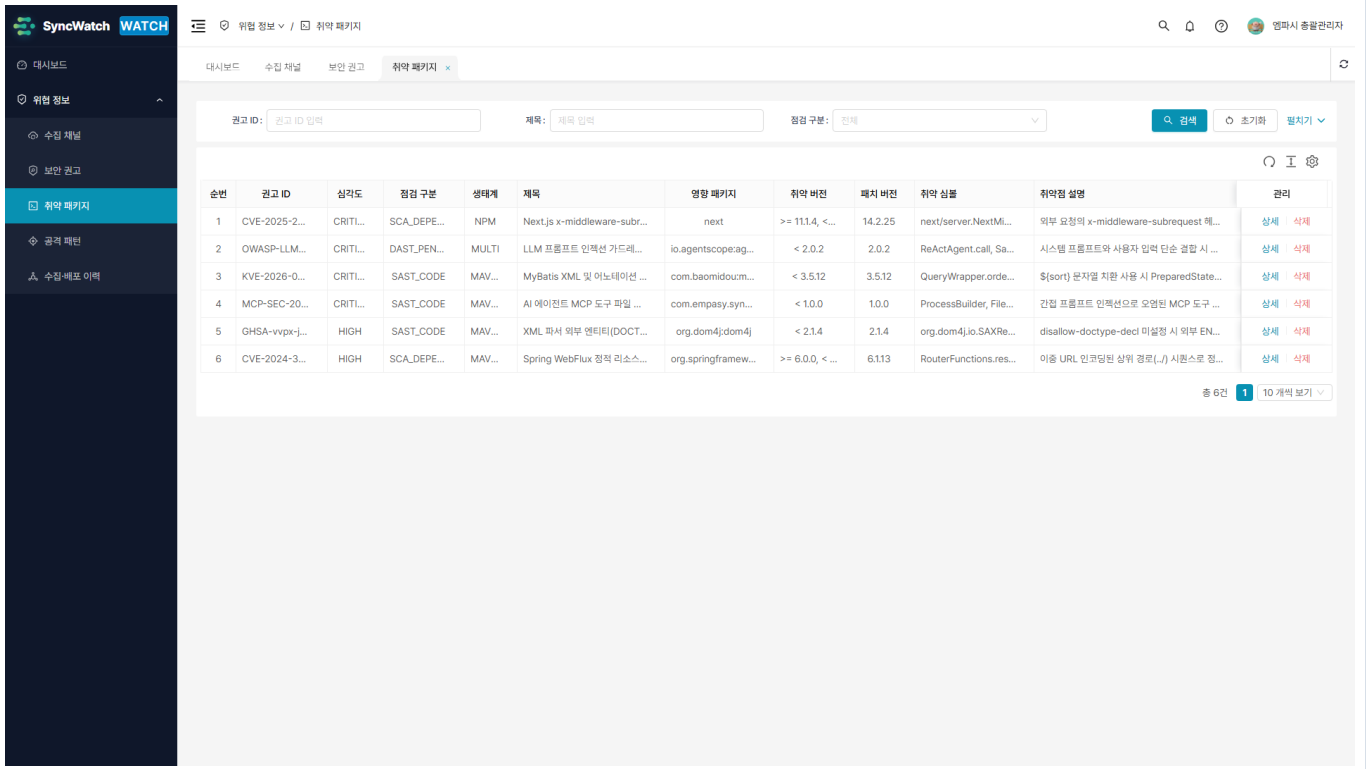
03 현업 개발자용 친절한 마크다운 조치 가이드 자동 생성

취약점의 위험 원리, 임시 완화 방법, 근본 패치 코드 예시를 한글 마크다운 가이드로 정리하여 개발자가 바로 이해하고 조치할 수 있게 돕습니다.

04 SyncVerse 코드 품질 감사기로 원클릭 전송

추출된 점검 기준(VerseAuditPack)을 SyncVerse로 즉시 배포하여 사내 모든 Git 저장소에 해당 취약점이 존재하는지 자동 스캔하게 합니다.

https://sync.empasy.io/watch/verse-rules



구동 화면 | SyncWatch 취약 패키지 및 코드 점검 기준 — 생태계별 패치 버전, 취약 심볼 및 SyncVerse 공급 규칙 (시연 데이터 기준)

실무 활용 보안팀이 영문 CVE 공지를 번역해 개발팀에 설명하느라 쓰던 시간을 없애고, 개발자가 바로 적용할 수 있는 정확한 패치 명세를 제공합니다.

운영팀용 API 차단 규칙 변환 및 공격·정상 샘플 사전 시험

활용 시점 : 새로 공개된 웹/API 해킹 기법(SQLi, RCE, SSRF, AI 프롬프트 공격 등)을 막는 실시간 가상 패치 규칙을 확인하고 SyncAPIM에 배포할 때 사용합니다.

주요 제공 기능

샘플 사전 시험 후 배포

01 HTTP 검사 위치(HEADER · URI · QUERY · BODY)별 정밀 탐지식 컴파일

공격 페이로드가 들어오는 정확한 HTTP 위치와 ReDoS-Safe 정규식, Restricted SpEL 방어 조건식, 구문 지문을 자동으로 생성합니다.

02 공격 샘플(Positive) & 정상 샘플(Negative) 샌드박스 자체 시험

만들어진 규칙이 실제 공격 페이로드는 정확히 탐지하고, 유사하게 생긴 정상 업무 요청은 정상 통과시키는지 화면에서 즉시 시험합니다.

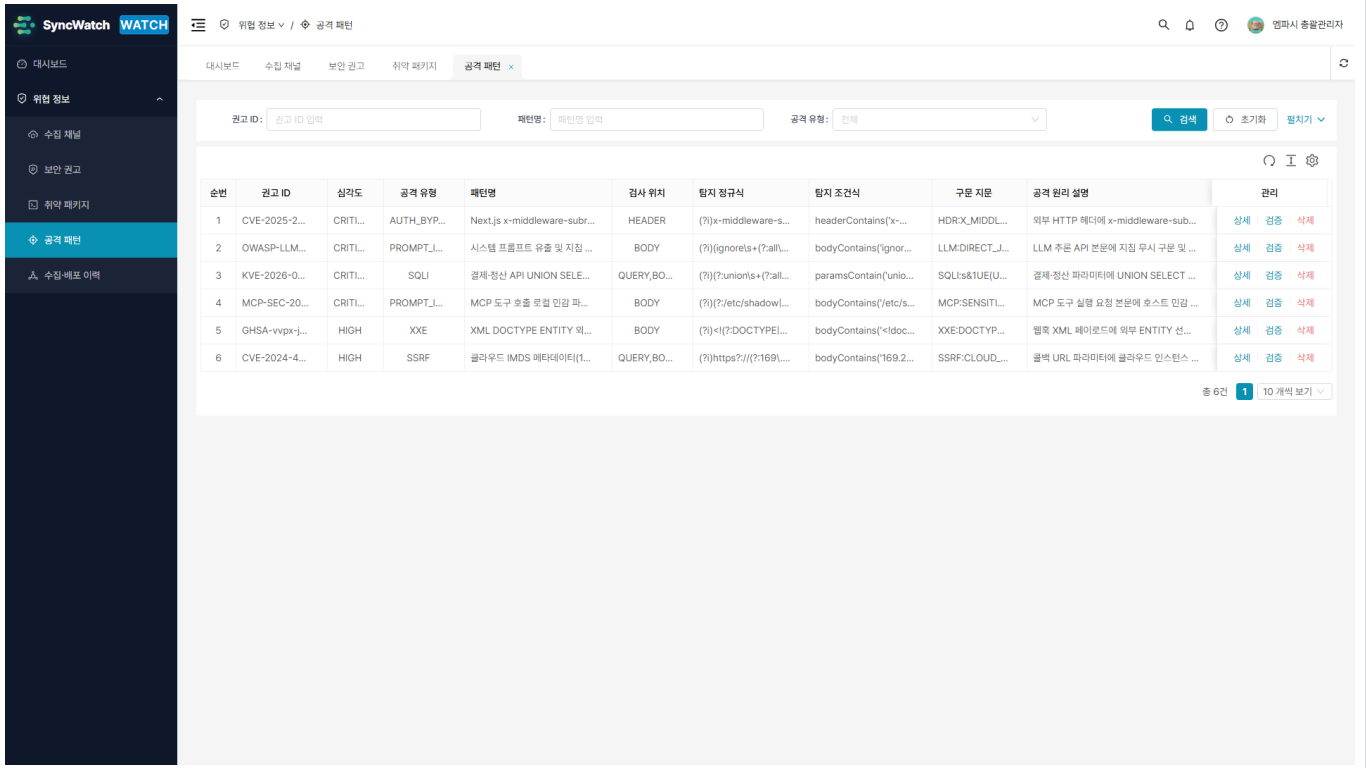
03 권장 조치 수준(즉시 차단 BLOCK / 감시 로깅 SHADOW) 자동 제시

위협 심각도와 검증 신뢰도에 따라 즉시 차단할지, 먼저 감시 모드로 운영할지 최적의 기본 정책을 제안합니다.

04 SyncAPIM 게이트웨이 무중단 배포 및 적용 피드백(ACK) 추적

검증이 끝난 방어 규칙(ApimDefensePack)을 SyncAPIM으로 전송하고, 게이트웨이 인라인 엔진에 몇 초 만에 반영되었는지 끝까지 추적합니다.

https://sync.empasy.io/watch/apim-rules



구동 화면 | SyncWatch 공격 패턴 시그니처 & 샌드박스 검증 — Restricted SpEL 방어식 및 정·오탐 테스트 결과 (시연 데이터 기준)

실무 활용 검증되지 않은 보안 룰 배포로 인한 서비스 장애를 막고, 수학적으로 안전성이 입증된 방어 시그니처만 운영 게이트웨이에 장전합니다.

5단계 외부 연결 안전 검사 및 공격·정상 샘플 사전 시험 통과 후 배포

외부에서 수집하는 보안 데이터 자체가 공격 통로가 되거나, 잘못된 방어 규칙이 사내 시스템을 멈추게 하는 일을 철저히 차단합니다.

1차 안전망 · 안전 수집 — 내부망 접근 사전 차단

5단계 SSRF 가드 및 스트림 크기·타임아웃 통제

외부 피드 수집 시 사설망(10.x, 192.168.x), 루프백(127.0.0.1), 클라우드 메타데이터(169.254.169.254) 접근을 미리 차단하고 DNS 재바인딩 공격을 방어합니다.

2차 안전망 · 샌드박스 — 위험 패턴 사전 걸러냄

ReDoS 복잡도 차단 및 공격·정상 샘플 사전 시험

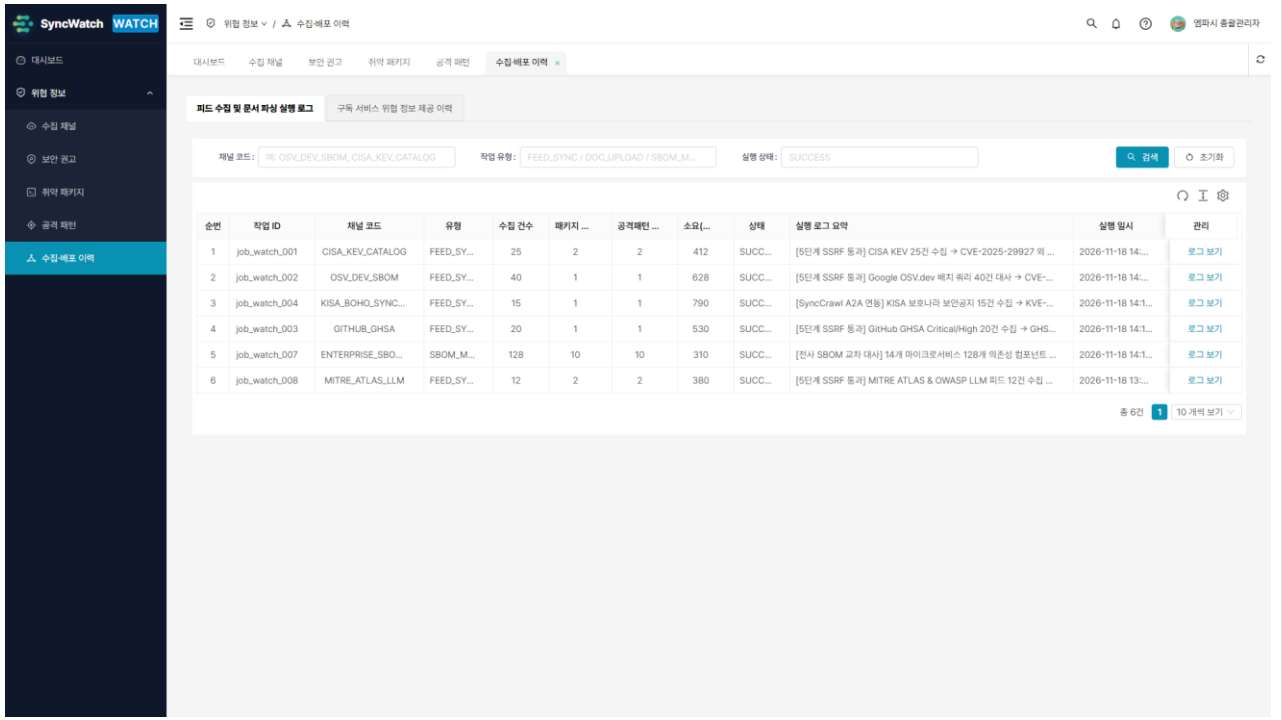
백트래킹 폭발을 일으키는 위험 정규식을 컴파일 단계에서 거부하고, 반드시 공격 샘플과 정상 샘플 양쪽 테스트를 모두 통과해야만 VERIFIED 등급을 부여합니다.

3차 안전망 · 양방향 추적 — 배포 완료 상태 추적

5단계 수집·컴파일 실행 로그 및 하위 시스템 ACK 감사

피드 수집 -> 파싱 -> 정규화 -> 듀얼 컴파일 -> 샌드박스 검증 전 과정을 밀리초 단위로 기록하며, SyncVerse·SyncAPIM의 실제 적용 완료 보고까지 양방향으로 확인합니다.

https://sync.empasy.io/watch/dispatches



구동 화면 | SyncWatch 5단계 수집 실행 로그 및 구독 서비스(SyncVerse·SyncAPIM) 양방향 배포 추적 (시연 데이터 기준)

안전 통제 — '수집은 안전하게, 규칙 검증은 깐깐하게, 배포 추적은 끝까지' 수행하여 전사 보안 자동화의 신뢰도를 완성합니다.

단독 위협 정보 포털로 쓰거나 SyncAPIM·SyncVerse와 방어 루프 연계

보안팀의 수작업 위협 모니터링 부담을 덜어주는 단독 포털부터, 탐지 즉시 방어까지 이어지는 자율 보안 루프의 핵심 두뇌로 작동합니다.

방식 A. SyncWatch 단독 도입 (기존 사내 시스템에 연결)

01. 전사 통합 보안 위협 인텔리전스(CTI) 브리핑 포털

국내외 8대 보안 채널을 한곳에서 한글로 모니터링하고, 우리 회사 기술 스택(Java, Vue, Python, Docker 등)에 영향을 주는 취약점만 즉시 필터링합니다.

02. 기존 사내 WAF 및 SIEM(Splunk/ELK)용 표준 보안 룰 내보내기

컴파일된 공격 패턴 정규식과 취약 패키지 목록을 JSON, SARIF 2.1.0, STIX 2.1 표준 포맷으로 내려받아 기존 보안 장비에도 활용할 수 있습니다.

03. 외부 보안 점검 보고서 및 수동 권고문 즉시 파싱

외부 보안 컨설팅 업체나 금융보안원으로부터 받은 취약점 보고서를 업로드하면 자동으로 코드 점검 기준과 방어 규칙으로 변환해 줍니다.

04. 폐쇄망 반입용 검증 완료 보안 룰 팩(Rule Pack) 생성

인터넷 연결망에서 수집·검증한 최신 방어 규칙 묶음을 망연계 솔루션을 통해 사내 폐쇄망으로 안전하게 반입할 수 있도록 지원합니다.

방식 B. SyncSeries 연계 확장 (MCP 표준 에이전트 협업)

SyncAPIM 연동 — **공격 패턴 시그니처 공급 -> 1분 내 실시간 가상 패치**

SyncWatch가 컴파일한 ApimDefensePack을 SyncAPIM이 즉시 수신하여 서버 재배포 없이 외부 해킹 트래픽을 인라인에서 바로 차단합니다.

SyncVerse 연동 — **취약 패키지·코드 기준 공급 -> 자동 코드 감사 & 패치 PR**

SyncWatch가 추출한 VerseAuditPack을 SyncVerse가 받아 전사 소스코드와 SBOM을 스캔하고 의존성 업그레이드 PR을 자동 생성합니다.

SyncCrawl 연동 — **동적 웹 렌더링 기반 KISA 및 보안 공지 무중단 수집**

일반 API가 없는 국내외 보안 공지 웹페이지는 SyncCrawl의 자가 치유 브라우저 에이전트와 협력하여 본문과 표를 깨짐 없이 수집합니다.

SyncETA 연동 — **신규 취약점 기반 모의해킹(DAST) 테스트 시나리오 공급**

새로 발표된 취약점의 공격 샘플(Probe)을 SyncETA에 전달하여 우리 서비스가 해당 공격에 안전한지 자동 회귀 테스트를 수행합니다.

유연한 도입 SyncWatch가 위협을 읽고 규칙을 만들면, SyncAPIM이 밖에서 막고 SyncVerse가 안에서 고치는 명확한 역할 분담으로 동작합니다.

며칠 걸리던 보안 공지 분석과 방어 규칙 준비를 분 단위로 앞당깁니다

보안 인력이 부족한 조직에서도 글로벌 대기업 수준의 24시간 위협 수집과 즉각적인 방어 룰 배포 체계를 갖출 수 있습니다.

공인 보안 피드 자동 수집
8대 채널 상시
OSV·GHSA·NVD·CISA·Nuclei·OWASP·MITRE·KISA

위협 공지 -> 방어 룰 변환
수일 -> 1분
듀얼 아티팩트 자동 컴파일러

방어 규칙 샌드박스 검증
샌드박스 검증
공격·정상 샘플 사전 시험

인바운드 수집 보안 검증
5단계 SSRF 가드
DNS Pinning 및 사설망 사전 차단

비교 항목	기존 방식 (AS-IS)	SyncWatch 적용 후 (TO-BE)	예상 개선 변화
보안 위협 모니터링	담당자가 매일 아침 KISA·NVD·GitHub 사이트를 돌아다니며 수기 확인	8대 글로벌·국내 보안 채널을 24시간 자동 수집해 단일 원장에 정규화	**모니터링 공수 90% 절감**
방화벽 차단 룰 작성	영문 권고문을 읽고 보안 엔지니어가 수작업으로 정규식 작성 (1~3일 소요)	공격 메커니즘을 자동 분해해 HTTP 위치별 정규식 및 SpEL 방어식 즉시 합성	**룰 작성 시간 95% 단축**
개발팀 취약점 전파	엑셀로 취약 라이브러리 목록을 정리해 메일 발송 후 수주간 수동 취합	패치 버전·취약 심볼·조치 가이드를 자동 추출해 SyncVerse 코드 감사에 직결	**패치 리드타임 단축**
차단 룰 안전성 검증	급하게 적용한 정규식 때문에 정상 서비스가 막히거나 CPU 과부하 발생	ReDoS 복잡도 차단 및 공격/정상 샘플 샌드박스 시험(정상 요청 통과) 통과분만 배포	**샘플 시험 후 반영**
조치 완료 여부 추적	룰을 전달한 뒤 실제 게이트웨이와 코드에 반영됐는지 수기 확인	SyncAPIM(가상 패치 완료) 및 SyncVerse(패치 병합 완료) 양방향 ACK 실시간 추적	**반영 이력 증적 보관**

기대 효과 보안 담당자는 단순 공지 검색과 정규식 코딩에서 벗어나, 전사 보안 전략과 핵심 의사결정에만 집중할 수 있습니다.

설치 직후 8개 채널 수집을 시작해 3주 내 전사 대응 흐름 구성

경량 컨테이너 구조로 설계되어 별도의 대규모 하드웨어 투자 없이 기존 보안·관제 서버에 바로 배포할 수 있습니다.

1. 현업 부담을 줄이는 4단계 점진 도입 절차

STEP 01 | 1주차
8대 보안 피드 연결 및 정규화 원장 구축
SyncWatch 설치, 5단계 SSRF 가드 진단 완료 및 8대 국내외 보안 채널 초기 동기화·정규화

STEP 02 | 2주차
사내 기술 스택 필터 및 듀얼 컴파일 검증
우리 회사 사용 생태계(Maven/NPM/Docker 등) 중점 규칙 컴파일 및 샌드박스 정·오탐 검증 가동

STEP 03 | 3주차
SyncAPIM & SyncVerse 양방향 자동 배포 연결
SyncAPIM 실시간 가상 패치 공급 및 SyncVerse 취약 코드·라이브러리 자동 감사 파이프라인 연동

STEP 04 | 4주차~
정기 위협 브리핑 및 양방향 조치 완료 감사
신규 CISA KEV / KISA 긴급 공지 실시간 Slack 알림 및 전사 취약점 조치 완료율(SLA) 리포트 운영

2. 권장 서버 하드웨어 사양 (온프레미스 / 클라우드 공통)

구성 구분	권장 CPU · 메모리 · 디스크 및 적용 대상
단독 구동 / 소규모	4 vCPU / 8GB RAM / 100GB SSD (8대 보안 피드 수집, 듀얼 규칙 컴파일 및 샌드박스 검증 충분)
전사 표준 운영형	8 vCPU / 16GB RAM / 200GB NVMe SSD (PostgreSQL 18.6 정규화 위협 원장 + Redis 7.4 동기화 락)
망분리 / 폐쇄망 구성	인터넷망 수집·검증 노드(4 vCPU/8GB) + 내부망 배포 노드(4 vCPU/8GB, STIX/SARIF 번들 반입)
통합 배포 시	SyncSeries 단일 서버 올인원 구성 또는 기존 SyncAPIM/SyncVerse 클러스터 내 컨테이너로 통합 배포 가능

3. 표준 기술 사양 및 호환 환경

기술 영역	적용 기술 및 지원 규격
백엔드 & 컴파일러	Java 25 (JDK 25), Spring Boot 3.5, Dual Artifact Rule Compiler, 5-Stage SSRF Guard, AgentScope Java
데이터베이스 & 캐시	PostgreSQL 18.6 (보안 권고·취약 패키지·공격 시그니처·배포 이력 표준 6단계 DB 스키마), Redis 7.4
지원 피드 & 표준 포맷	OSV.dev, GitHub GHSA, NVD CVE 2.0, CISA KEV, Nuclei YAML, OWASP CRS, MITRE ATLAS, KISA, STIX 2.1, SARIF 2.1.0
프론트엔드 콘솔	Vue 3.5, TypeScript 5, Vite, Vben Admin (대시보드·수집 채널·보안 권고·취약 패키지·공격 패턴·배포 이력)

도입 지원 SyncWatch 하나를 더하는 것만으로 사내 개발 파이프라인과 운영 API 게이트웨이가 매일 최신 글로벌 보안 지능으로 무장됩니다.

EMPASY SYNCSERIES · SYNCWATCH

새로 발표되는 보안 취약점을 빠르게 파악해 사내 방어 기준으로 옮기는 일, SyncWatch가 보안팀과 개발팀의 대응 부담을 덜어 드립니다.

라이브 데모 포털(https://sync.empasy.io)에서 8대 보안 피드 수집 현황과 듀얼 방어 규칙 샌드박스 검증 화면을 직접 확인해 보세요.

01. 줄글 공지가 아닌 즉시 작동하는 방어 규칙

읽고 해석해야 하는 보안 뉴스 대신 개발팀이 바로 쓸 패치 기준과 운영팀이 바로 쓸 차단 시그니처를 자동으로 만들어 드립니다.

02. 공격·정상 샘플 샌드박스 사전 검증

모든 자동 생성 규칙은 공격 샘플과 정상 샘플을 이용한 자체 샌드박스 테스트를 통과한 뒤에만 안전하게 공급됩니다.

03. 탐지부터 패치 완료까지 양방향 상태 추적

규칙을 전달하는 데서 끝나지 않고 SyncAPIM과 SyncVerse에서 실제로 방어와 패치가 반영되었는지 끝까지 확인합니다.

라이브 데모 체험 : https://sync.empasy.io | 문서·제안서 포털 : https://doc.empasy.com
도입 상담 및 2주 시범 적용(PoC) 문의 : 주식회사 엠파시 솔루션아키텍처팀 | biz@empasy.io