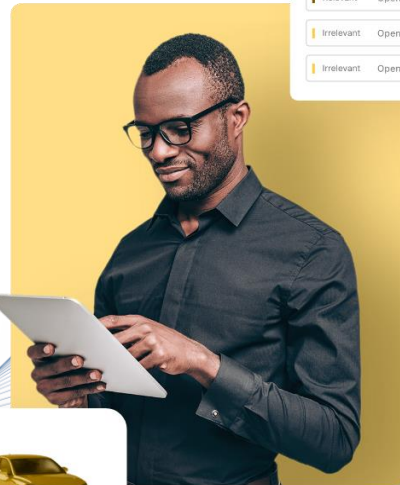


CSMS 관리 솔루션

(바이너리기반 Cyber Security Management System)

제품소개서



CVE-2020-15889

Relevant	OpenSSI 1.0	9.2	InfoPlaySys...
Irrelevant	OpenSSI 1.0	9.2	Telematics
Irrelevant	OpenSSI 1.0	9.2	ECU



CO**Corporation ON** by **TECH**nology



CONTENTS

1. CSMS 관리체계 이해
2. Cybellum 제품 소개
3. Cybellum 기본기능

Extreme Engineering

CSMS 관리체계 이해

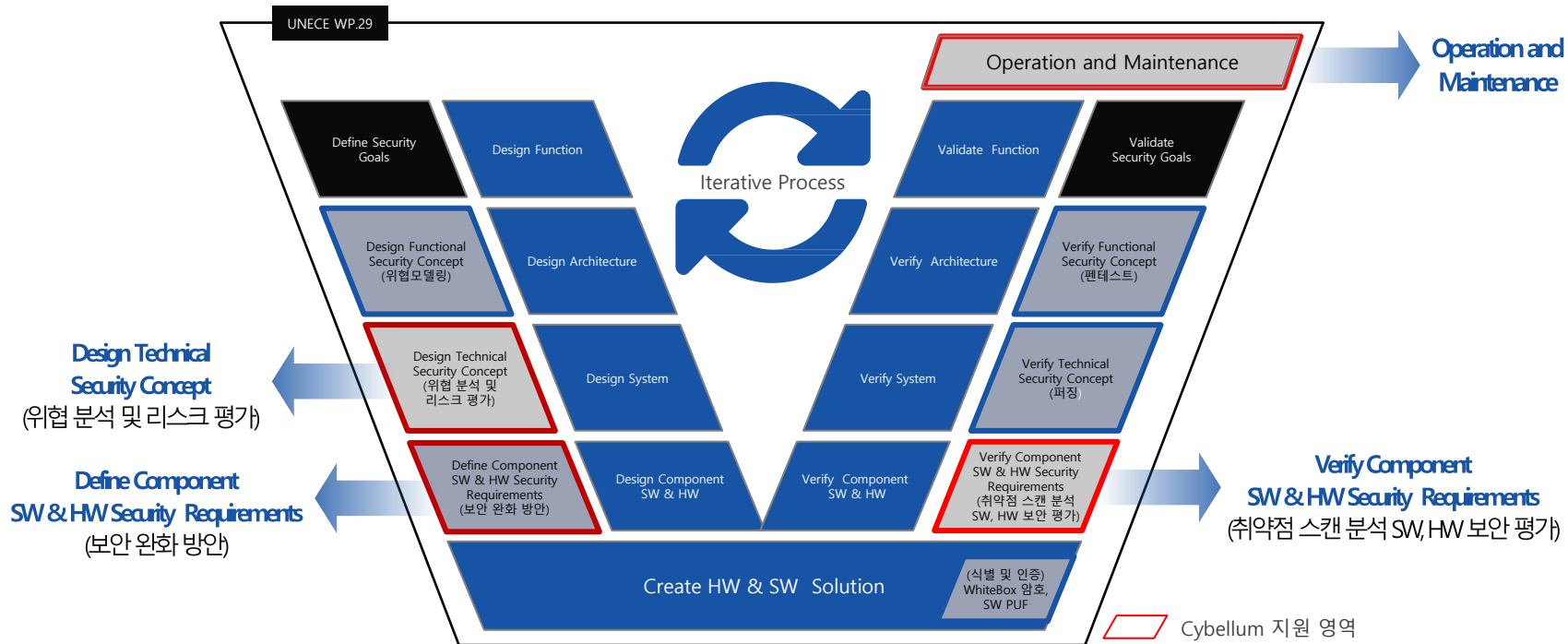


COrrporation ON by TEChnology | 쿤텍

© 2024. COONTEC Co., Ltd. All rights reserved.

01

01 Lifecycle 전반에 걸친 보안



02 CSMS(Cyber Security Management System)란?

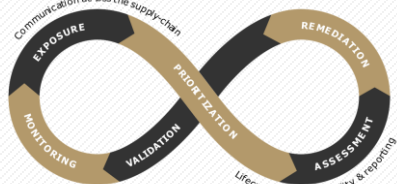
CSMS란 차량의 (E/E)시스템의 전체 생명주기 동안 사이버보안 위협에 대한 보장을 목표로 하는 체계

개념 단계
사이버 보안 위협 식별
보안위험 평가
예비 아키텍처 설계

개발 단계
Mitigation 결정
보안 요구사항 도출
설계 구현, 통합 검증

양산 후 폐기까지
사이버 보안 위협 식별
보안위험 평가
예비 아키텍처 설계

최신 위협 및 취약점 정보 TARA 기반의 위협 보안 대응 체계



ISO/SAE 21434 기반 산출물



사이버보안
위협 정보 수집



취약점
정보 제공



사이버보안
이벤트 대응



차량
모니터링



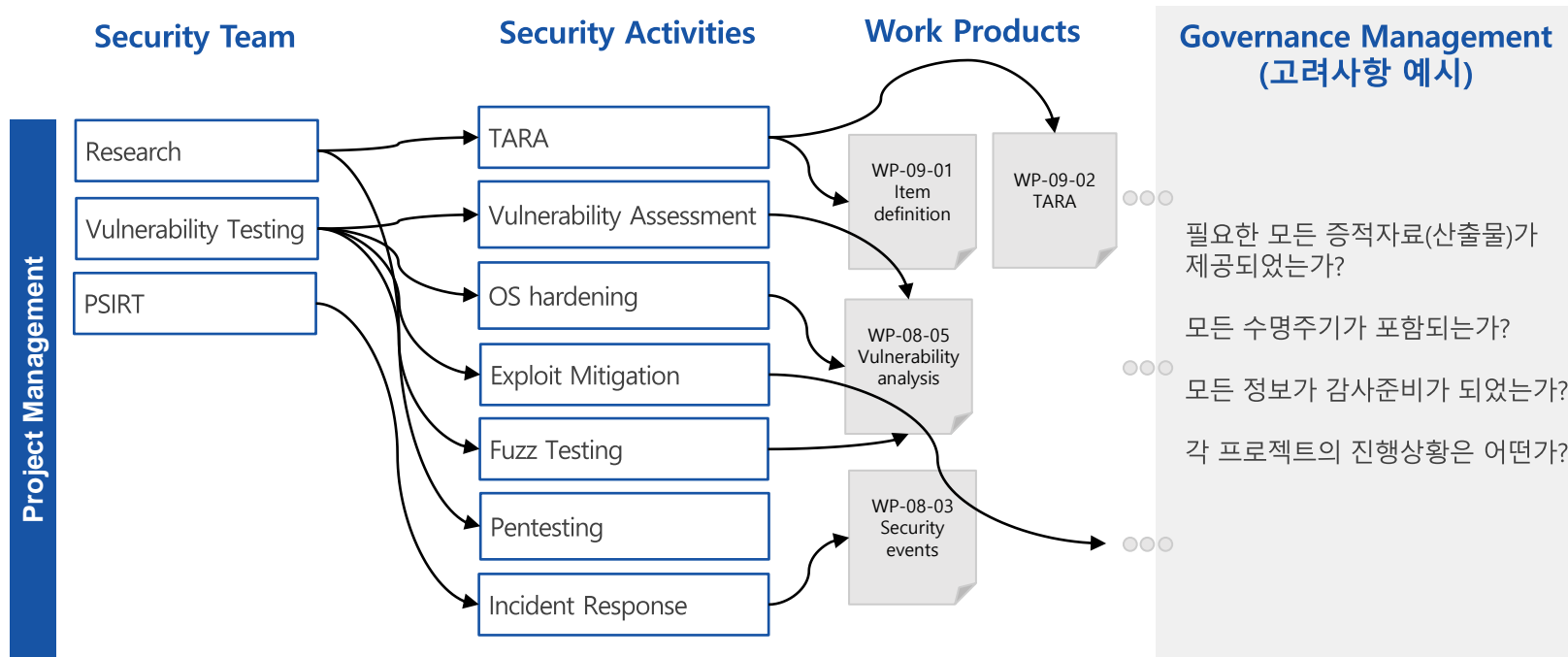
사이버보안
비용 절감

다크웹, 딥웹 위협 정보 수집과
분석을 통해 최신 위협 정보

알려진 취약점 정보(CVE + 공개
DB)를 기반으로 취약점 식별 정보
와 대응 방안

제조사 제공되는 최신 취약점
정보와 패치 버전 정보를 제공

출시된 모든 차량의 바이너리
를 모니터링하고 최신 위협 정
보를 매핑하여 정보제공



04 Cybellum CSMS 지원사항

The Product Security Platform

하나의 플랫폼에서 전체 보안 라이프사이클을 지원



전체 제품 개발 라이프 사이클과 동기화된 하나의 통합 보안 플랫폼



규정 준수 속도 향상



완전 자동화 및 확장 가능



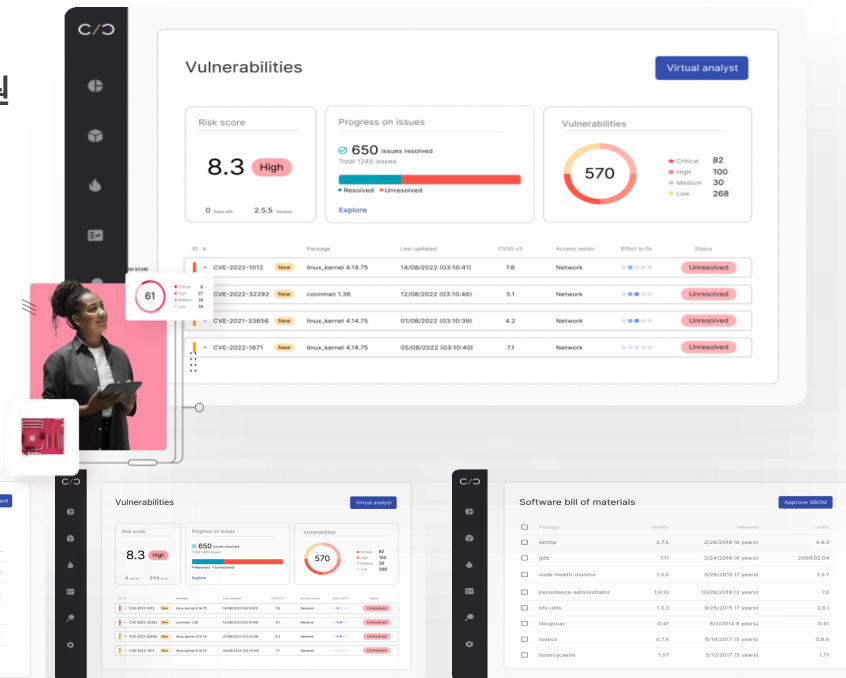
모든 릴리스, 제품 또는 구성 요소에 대한 지속적인 평가 가능



단순한 탐지가 아닌 위험 관리 및 완화 가능



자동차 산업에 맞는 지원



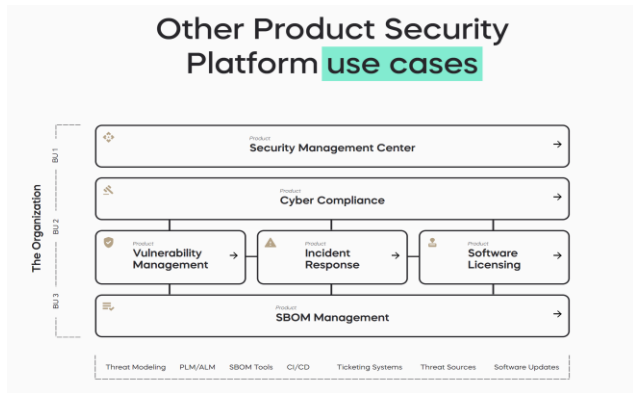
전체 보안 관리

오픈소스 라이선스 관리

취약점 관리

SBOM 및 자산 관리

05 Cybellum 이용한 CSMS 구축 사례 – LG 전자



CASE STUDY LG Electronics

C/O CYBELLUM



Cybellum은 하나의 플랫폼으로
CSMS 관리의 효율성을 증가시켜 줍니다.

Sungho Hwang | Cybersecurity Analyst Team Leader -LG

LG VS' achievements

Since implementing the Cybellum's Product Security Platform as its centralized solution for cyber security operations throughout the life cycle, LG VS is achieving the following benefits:

- ✓ The VTA process is now more streamlined, since the technical reports - product configuration, vulnerability analysis, vulnerability monitoring and incident response are all automated using the Cybellum Platform.
- ✓ Product cybersecurity information is always available across the company's diverse projects.
- ✓ SBOMs are now always available as they are automatically created.
- ✓ It is now 7x times faster to create SBOMs.
- ✓ More than 50% of vulnerabilities are automatically triaged as irrelevant, saving days of work.

Extreme Engineering

Cybellum 제품 소개

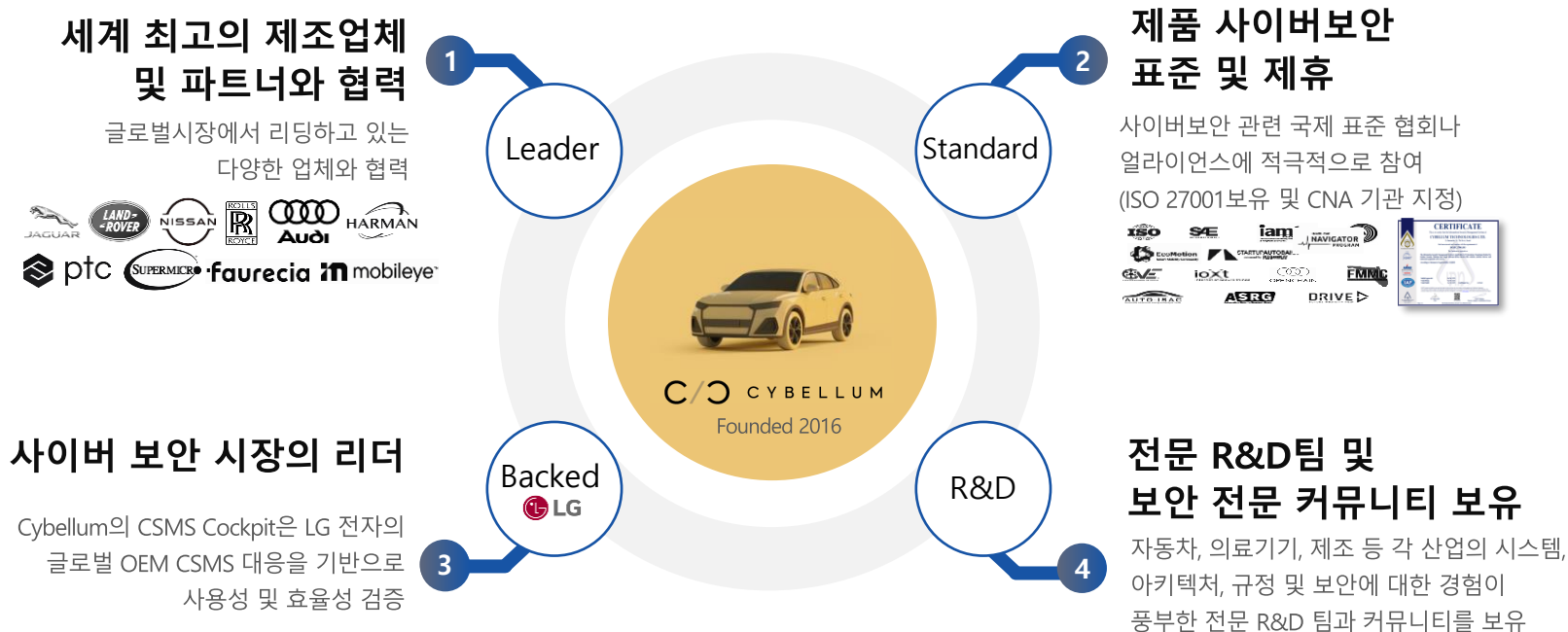


02

COrrporation **ON** by **TE**chnology | 쿤텍

© 2024. COONTEC Co., Ltd. All rights reserved.

01 Cybellum 소개



02 Partners & Customers

“다수의 대형 자동차 글로벌 고객사들은
사이버보안 대응을 위해 Cybellum을 선택”

CSMS 체계 구축을 위한 플랫폼 선정



03 Cybellum 특장점



디지털 트윈(Digital Twin) 기술

사이버상에 복제된 자산을 대상으로
모의테스트(정적 분석, 동적 분석)를 통해 결과에
대한 **정확한 예측 가능**



지속적인 영향 기반 평가

자동차 사이버 위험 정보를 기반으로 영향
분석을 수행하고 실시간 모니터링 하여
**소프트웨어의 사이버 보안 위험을 식별 &
지속적 평가**



컴플라이언스 준수 지원

자동차 국제 표준 지원(WP29, ISO/SAE 21434)
자동차 코딩룰 표준 검출 지원
(MISRA, CERT C, AUTOSAR, IEC 62443 등)
SBOM 점검 지원(SDPX, Cyclond DX 포맷 지원)



CSMS 관리 기능 제공

CSMS에 특화된 플랫폼을 통해 사이버 보안
관리 시스템을 자동화하여 차량이 디지털
보안을 유지하고 사이버 보안 규정을 완벽하게
준수하도록 보장

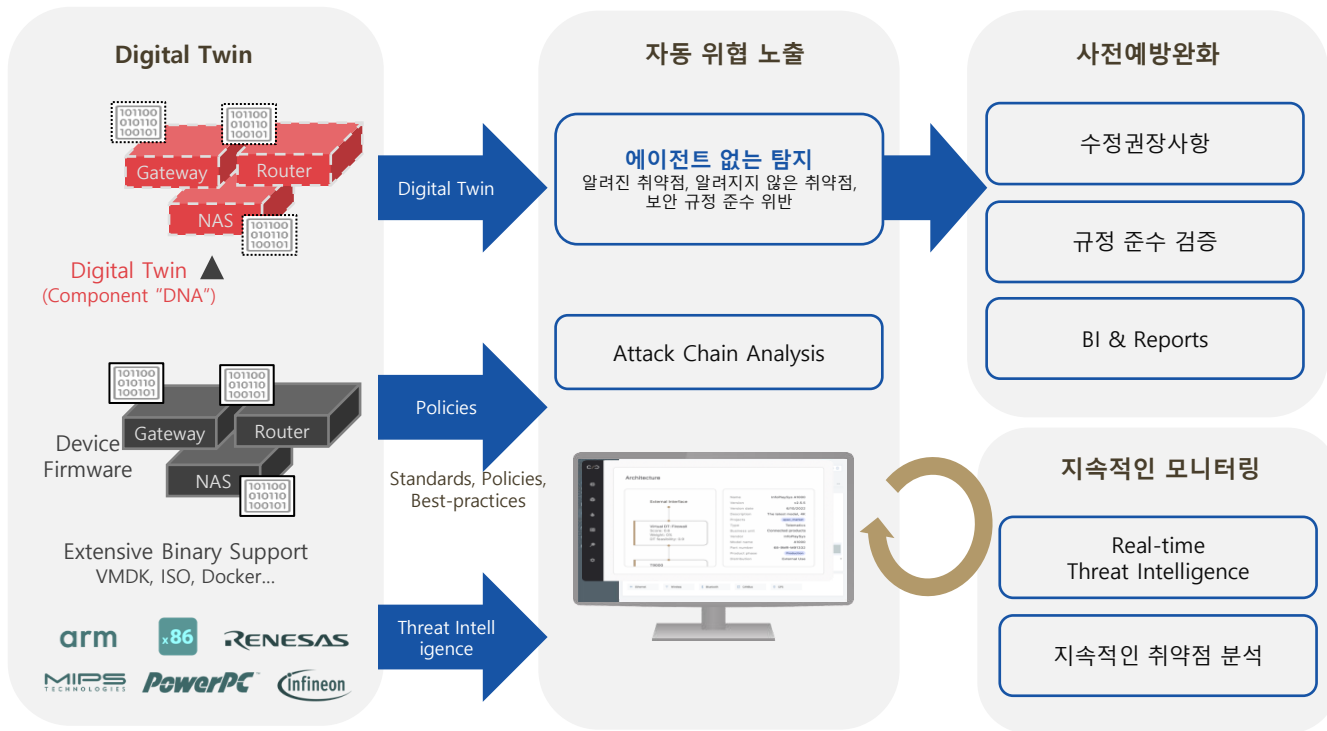


Off-device solution

별도의 에이전트가 필요 없이 웹UI를 통해
바로 분석이 가능
(On-Premise)

04 Cybellum 아키텍처

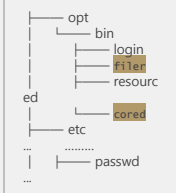
Cyber Digital Twins™이란?



05 분석기술 - SBoM(Software bill of materials)

HW 및 SW 전체 구성요소(Bill of Materials) 스캔을 통해 취약점의 실제 영향을 필터링하는데 필요한 전체 구성 정보를 제공

```
...PK.....O".0
[D.\S.....\A...
write_alloc.d.XX
711.020/bootload
er-walleye-mw899
8-002.0078.00.im
gUT.....VJ...V]ux
.....2.....S.....
t.....@B.Q...
<.@.u6...h...IxeCB
.hm$...y.f...Z.U
.[@.....@
y((.....j.A8..C.
7...n2.....p...
~.....3
.ef.:buf_synd.c.
..=..+.mc+*...E
n.h.9.I...x...Z
...[{<.A.G]...
.y$.a...?.....Y
...writer_disk0.y
d..wyy...75r.J.-
.y....PQ...*...<
>..d...f Y[...e
...?].;Bxg...
...
```



- 고컨텍스트 기반 협력적 필터링을 적용한 다단계 감지 엔진으로 소프트웨어 구성 요소 감지
 - 기능이름, 문자열, 디렉토리 구조, 파일유형, etc...

- 고유한 자동화 된 다중 요소 스코어링 메커니즘

- 바이너리를 알려진 패키지 전용 DB와 비교
- 광범위한 커버리지
 - 플랫폼 독립적 탐지(다양한 아키텍처 적용)
 - 중첩 탐지(정적으로 컴파일 된 라이브러리)식별
 - 스트레스 감지(수정 및 부분 난독화처리된 바이너리)

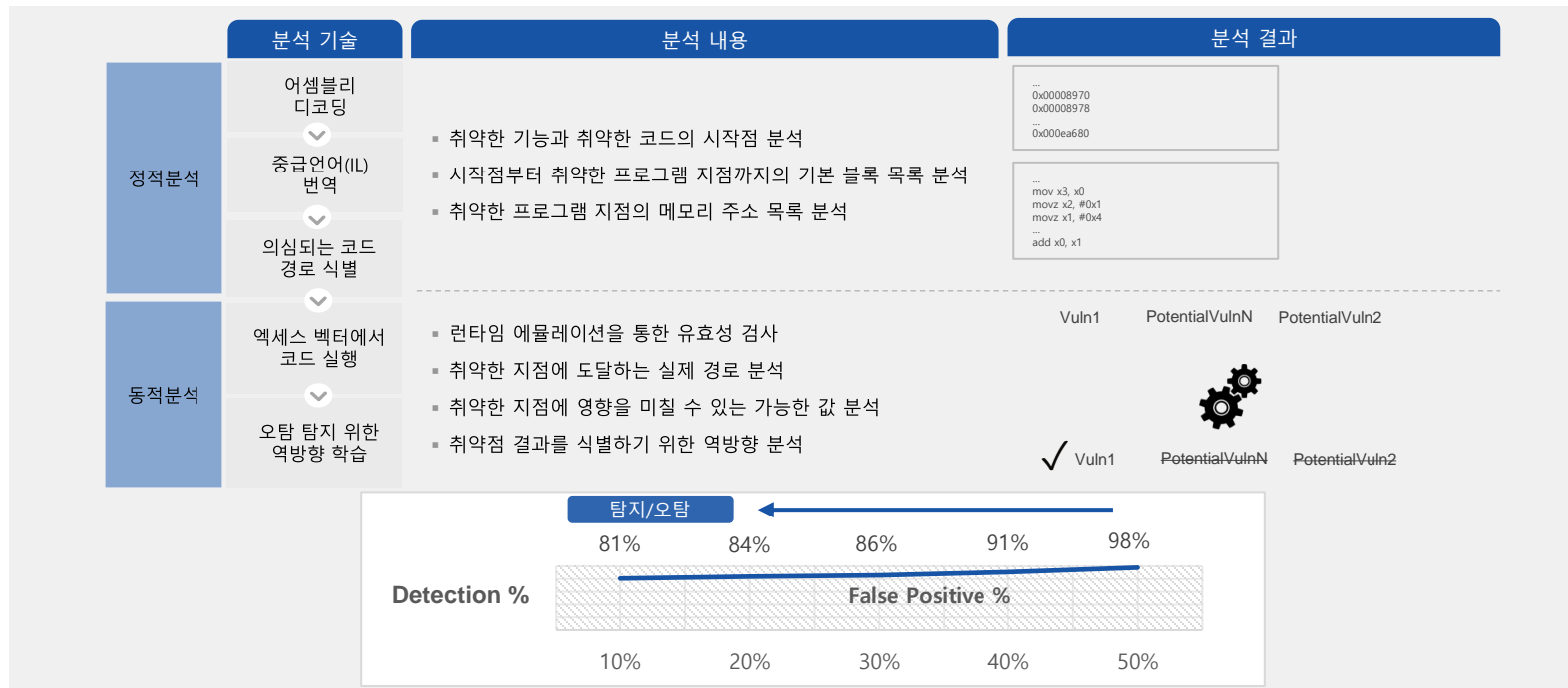
20 different attributes				
	File Names	Function Names	Strings	...
	9.5	8.7	9.8	

- 컨텍스트 식별 항목

CPU architecture	특정 CPU 아키텍처 및 word-length에만 영향을 미치는 취약점 식별
Unused interface	해당 펌웨어에서 사용되지 않은 인터페이스의 취약점 식별
Disabled kernel modules	비 활성화된 커널 모듈의 취약점 식별
OS vs. package-specific patches	전체 OS가 업데이트된 경우에만 적용되는 취약점 식별
Static libraries	정적으로 링크되어 라이브러리 코드의 일부만 장치에 존재하는 경우, 실제 취약한 코드가 존재하는지 식별
Code usage	취약한 API 가 존재하지만, 호출되지 않거나 사용되지 않는 경우
Unused commands	펌웨어에 설치되지 않은 특정 명령(command)에만 영향을 미치는 취약점 식별

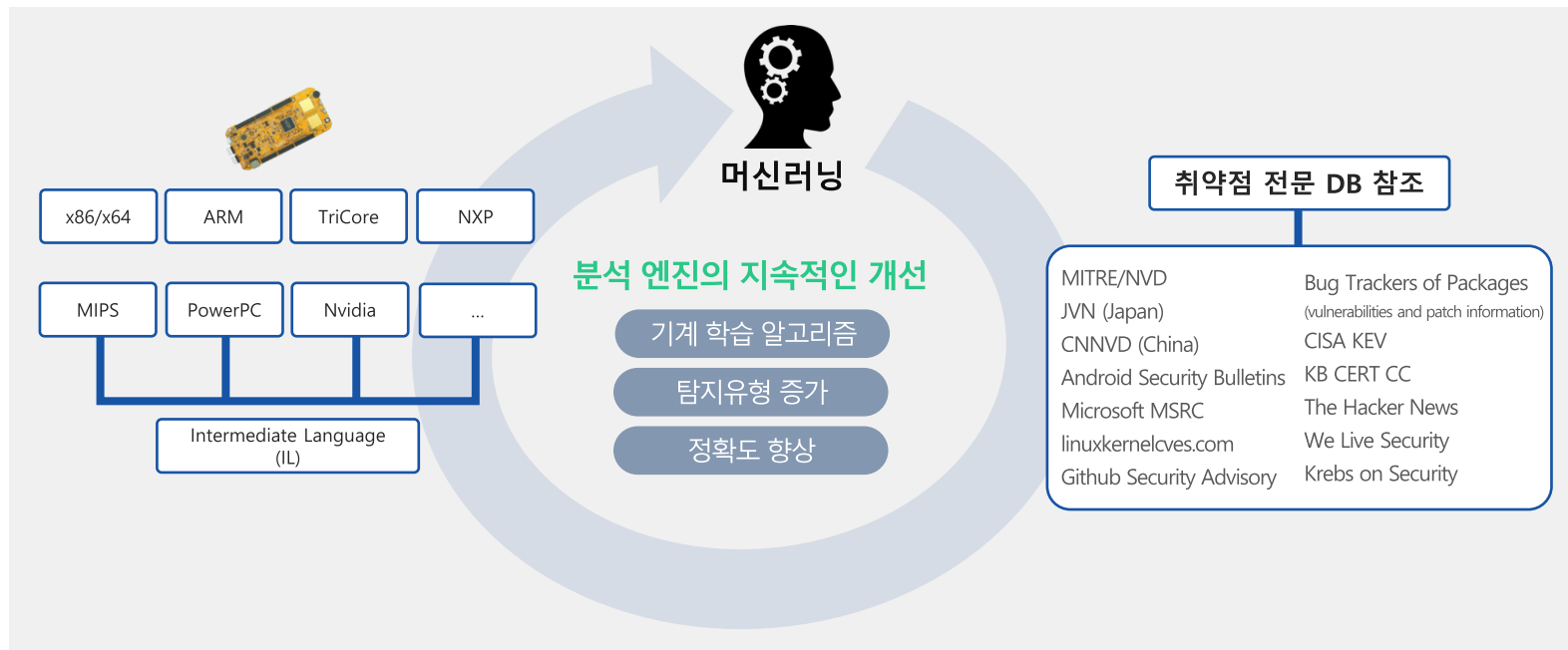
05 분석기술 – 분석 프로세스

고도화된 기술의 정적, 동적 분석엔진을 통해 바이너리 코드만으로 정확하고 상세한 보안 위험 탐지



05 분석기술 – 머신러닝 기반 분석 엔진

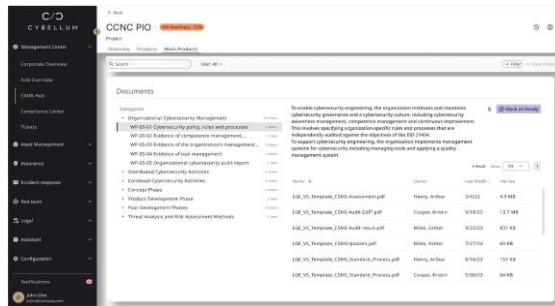
다양한 플랫폼의 바이너리 코드를 머신러닝 기반 분석엔진과 최신 취약점 DB를 참조하여 자동화된 분석을 실행하여 소프트웨어의 사이버 보안 위험을 식별 및 분석하여 사용자에게 정확한 결과를 제공합니다.



06 CSMS 특화 관리기술 – Cybellum CSMS Cockpit

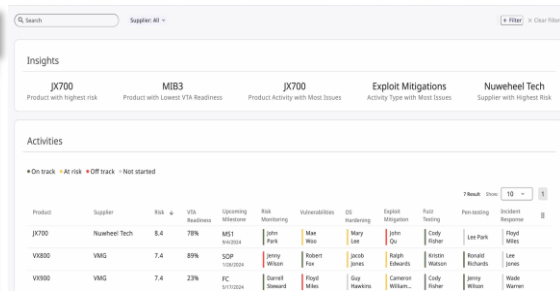
CSMS Cockpit은 제품 보안을 위한 제어 센터 역할을 하여 자동차 제조업체가 보안 위협을 신속하게 평가하고 해결할 수 있도록 하며, ISO/SAE 21434 기반의 관리 프로세스를 통해 국제 표준을 준수할 수 있도록 지원

CSMS Management



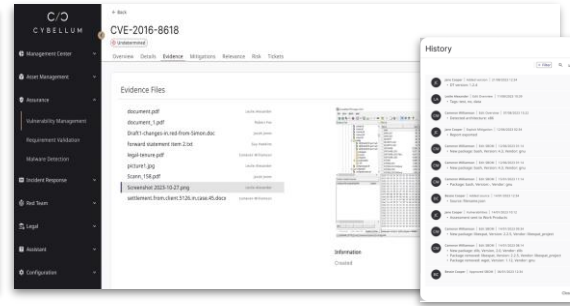
- 각 챕터 요구사항별 관련 정보 확인 가능
- ISO/SAE 21434 프레임 워크에 맞는 CSMS 산출물 제공

Automotive Compliance



- 각 제품별 공급자, 리스크 점수, 마일스톤 제공
- 각 보안 활동별 담당자 지정
- 전반적인 인사이트 제공

End-to-End Traceability



- 검출된 취약점과 관련된 파일 리스트 제공 및 상세 내용 제공
- 분석 결과에 대한 이력관리 제공

07 타솔루션 vs Cybellum 특징 비교

Asset & Findings Management

	C/O CYBELLUM	Other
OSS library detection	✓	✓
CVE detection	✓	✓
Commercial & proprietary packages detection and management	✓	
HW BOM & interfaces detection	✓	
Licensing info detection	✓	✓
Microcontroller support (e.g. MIPS, Renesas, TriCore)	✓	
OS support (e.g. QNX, Android, Autosar, RTOS)	✓	✓
SBOM autofix & approval	✓	
PII, credentials, cryptography, OS config., control flow	✓	
EPSS score and percentile data	✓	
APIs + integration with CI/CD, Ticketing, PLM, 3rd party SCA tools	✓	
Multiformat SBOM import/export + VEX reporting	✓	

Security Activities

	C/O CYBELLUM	Other
Remediation recommendations	✓	✓
Bulk mitigation suggestions	✓	
Multi-source threat intelligence gathering	✓	✓
TARA & OTA integration	✓	
Risk assignment based on customer/industry standard rules	✓	
Automated triaging of vulnerabilities (VM Co-Pilot)	✓	
Coding best practices validation (MISRA, CERT-C, etc)	✓	
Industry standards and organizational policies validation and enforcement	✓	
Multi-version/branch assessments and progress tracking	✓	
Coding weaknesses detection & management	✓	
Post-SOP security monitoring, investigation & reporting	✓	✓

Risk & Compliance Management

	C/O CYBELLUM	Other
Custom Management Dashboards	✓	
CSMS Cockpit (built-in security & compliance progress tracking)	✓	
OSS licensing policy management, validation and enforcement	✓	
Automated ISO 21434 work-product report generation, document upload and compliance readiness tracking	✓	
System of system representation & risk calculation	✓	

08 Cybellum 지원범위

유형	항목		유형	항목	
지원 OS	<ul style="list-style-type: none"> Linux <ul style="list-style-type: none"> Automotive Grade Linux (AGL) Android QNX NetBSD Windows server and client OSes <ul style="list-style-type: none"> Windows Mobile 	<ul style="list-style-type: none"> FreeBSD FreeRTOS Proprietary RTOS RIOT Fuchsia OS OSEK OS VxWorks 외 다수 	아카이브 / 압축파일 포맷	<ul style="list-style-type: none"> 7-Zip (.7z) ARJ (.arj) bzip2 (.bz2) Compress (.Z) cpio (.cpio) Gzip (.gz) LZ4 (.lz4) LZMA (.lz) Pack200 (.jar) RAR (.rar) TAR (.tar) UPX (.exe) XAR (.xar) 	<ul style="list-style-type: none"> XZ (.xz) ZIP (.zip, .jar, .apk, others) LZH (.lzh) DEFLATE Electron archive (.asar) AR archive Base64 Irzip lzip Lzop OTF rzip Stfflit
펌웨어 포맷	<ul style="list-style-type: none"> Android (boot, sparse image, backup file) Intel HEX SREC U-Boot Ambarella (.a9s, .a9h, romfs) Dahua DJI TPLink WR702n image 	<ul style="list-style-type: none"> TRX UEFI firmware VBF VxWorks ROS Xerox DLM Arris firmware Juniper firmware Kosmos firmware Cisco firmware 외 다수 	지원 아키텍처	<ul style="list-style-type: none"> Renesas <ul style="list-style-type: none"> V850, SuperH Power PowerPC ARM Cortex-M ARM Cortex-A ARM Cortex-R 	<ul style="list-style-type: none"> MIPS NXP x86 x64 NVIDIA AGX <ul style="list-style-type: none"> Xavier Infineon <ul style="list-style-type: none"> TriCore Sparc 외 다수
파일 시스템 / 디스크 이미지	<ul style="list-style-type: none"> ext2/3/4 ISO 9660 / UDF (.iso) JFS, JFFS2, YAFFS Macintosh HFS, APFS QEMU Copy-On-Write (.qcow2) QNX—EFS, IFS RomFS UBIFS Windows Imaging (WIC) Btrfs 	<ul style="list-style-type: none"> CramFS DOS MBR minix Reiserfs SquashFS XFS NetBoot image (.nbi) VirtualBox VDI (.vdi) VMware VMDK (.vmdk, .ova) 	지원 언어	<ul style="list-style-type: none"> Assembly BASIC C C++ Delphi Go Qt 	<ul style="list-style-type: none"> Haskell Java Lisp OCaml Objective-C Rust Swift 외 다수

Extreme Engineering

Cybellum 기본기능



COrrporation ON by TEChnology | 쿤텍

© 2024. COONTEC Co., Ltd. All rights reserved.

04

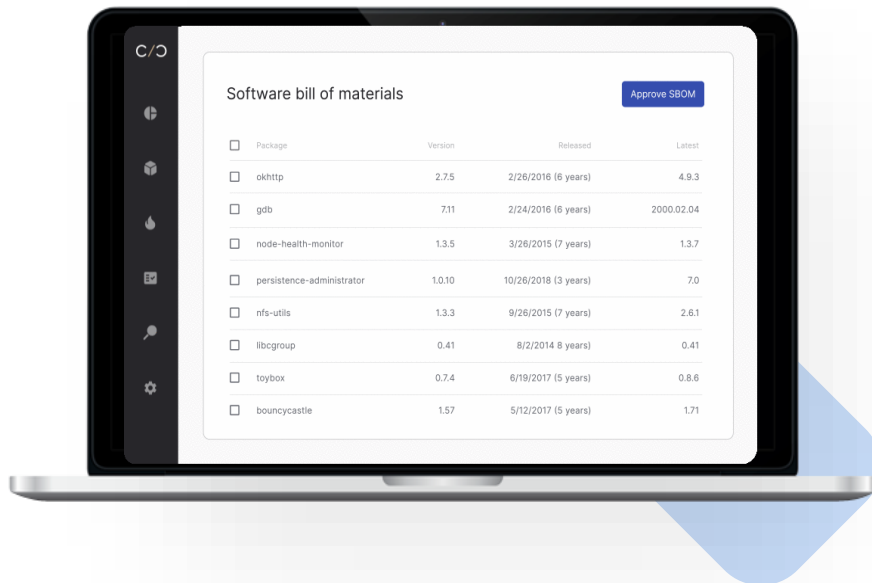
01 Cybellum 기능 – SBOM 관리



SBOM 및 자산 관리

모든 프로젝트 및 제품 라인에 대해
SBOM 저장소를 구축하고 검증을 통해
프로세스에 따라 유용하게 관리할 수 있습니다.

- ▶ SBOM 정보, 라이브러리 정보, 라이선스, 암호화 정보, URL, 버전 정보 등 제공
- ▶ 생성 및 병합, 검증, 승인, 협업 관리 및 조정 가능



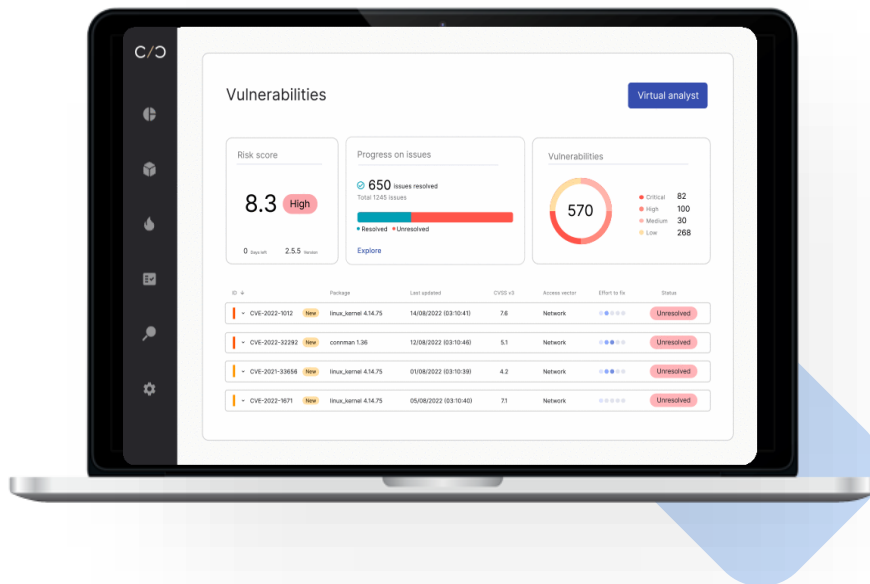
01 Cybellum 기능 – 취약점 관리



취약점 관리

제품의 취약점을 자동으로 감지하고
우선순위 지정을 통해 취약점 조치 속도를
높여 제품 보안 상태를 높입니다.

- ▶ CVE 및 CWE 취약점 상세 정보, Risk Score, CVSS 점수, EPSS 점수, 취약점 조치 권고 사항, 취약점 조치 유무 등 제공
- ▶ 지속적인 위험 모니터링 가능



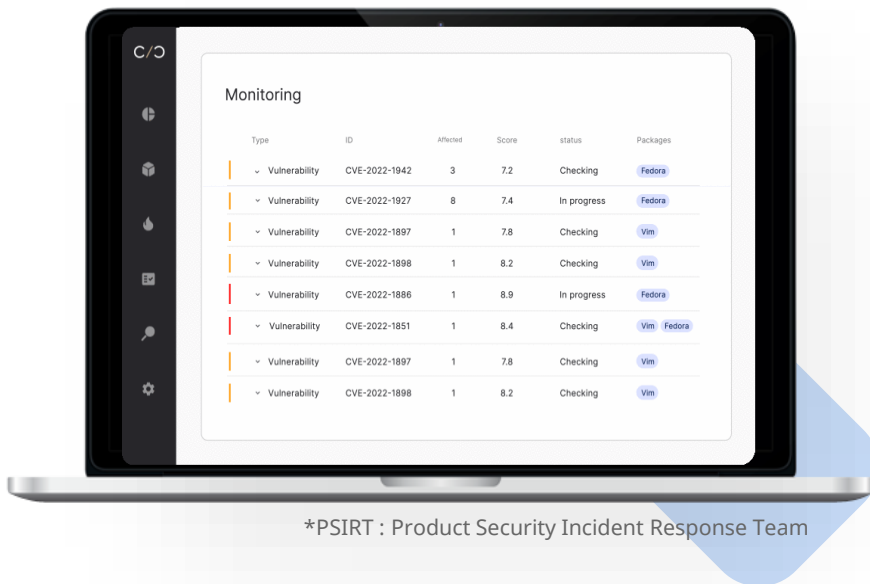
01 Cybellum 기능 – PSIRT 관리



PSIRT 관리

지속적으로 보안 취약점에 대해 모니터링할 수 있도록 제공하여 제품 출시 이후에도 빠르게 조치할 수 있도록 많은 정보를 제공합니다.

- ▶ 특정 취약점의 영향을 받는 프로젝트 확인 가능
- ▶ 취약점 영향도, 취약점 조치 유무상태, 패키지명 등 제공



*PSIRT : Product Security Incident Response Team

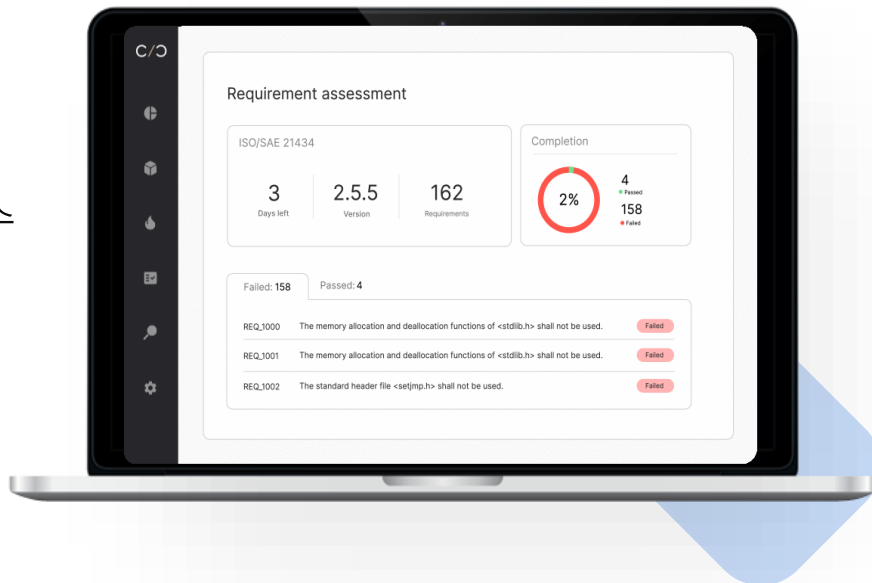
01 Cybellum 기능 – 컴플라이언스 관리



사이버보안 컴플라이언스 관리

각 산업별 컴플라이언스 (WP. 29, ISO/SAE 21434, MISRA C, CERT C, AUTOSAR 등) 준수여부 자동 확인 및 자동차 사이버 보안 표준 맞춤화 리포트를 통해 컴플라이언스를 빠르게 준수할 수 있습니다.

- ▶ 50개가 넘는 표준에 대한 사전 구축된 Cybellum 매핑 데이터베이스를 통해 원클릭으로 규제 보고서 추출이 가능 (WP 29, ISO/SAE 21434, FDA 등)



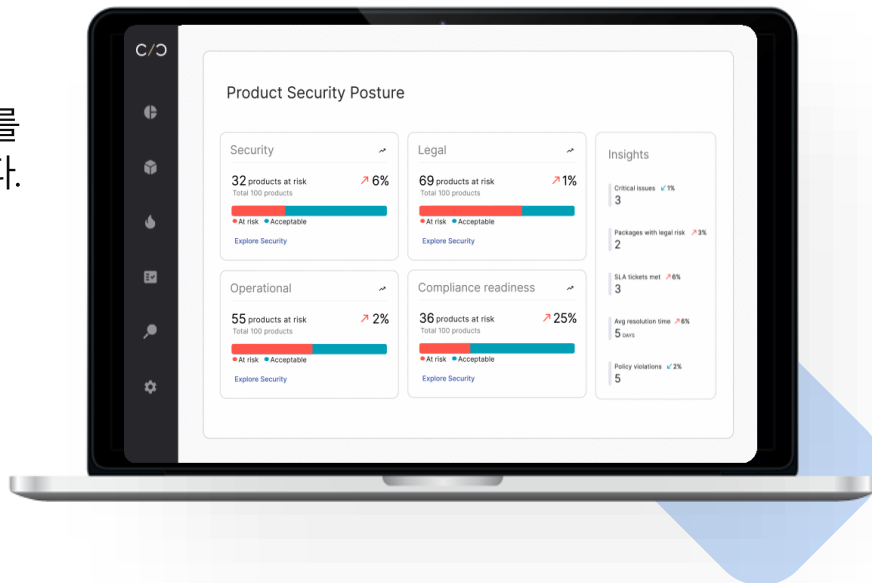
01 Cybellum 기능 – 보안 관리



보안 관리

제품 보안 관리자를 위해 중앙 집중식 대시보드를 사용하고 있으며, 가장 중요한 문제를 빠르게 파악할 수 있도록 인사이트를 제공합니다.

- ▶ 중앙 집중식 대시보드 제공, 관리자 관리 기능 제공



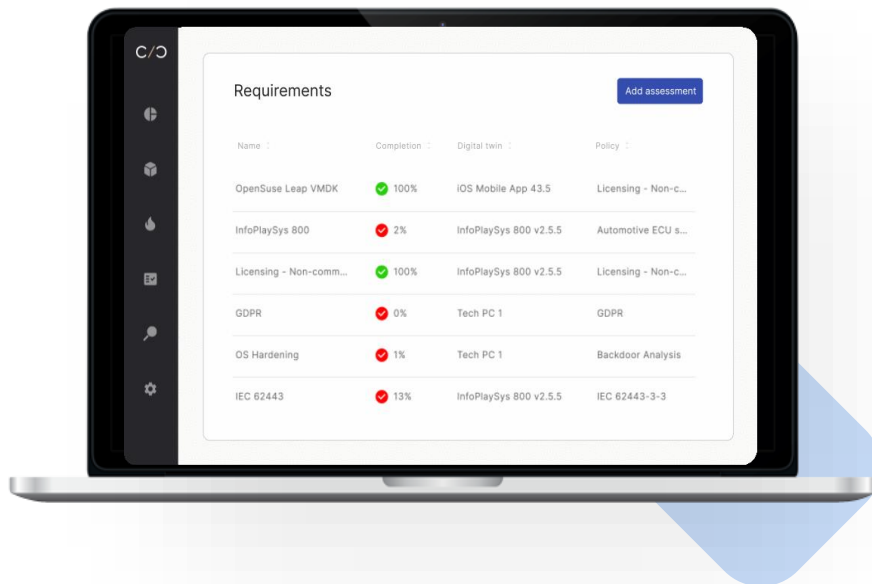
01 Cybellum 기능 – 오픈소스 라이선스 관리



오픈소스 라이선스 관리

소프트웨어 라이선스를 확인 및 관리할 수 있으며, 라이선스 정책을 통해 오픈소스 법적 위험을 줄일 수 있습니다.

- ▶ 소프트웨어내 오픈소스 라이선스를 식별, 사전 라이선스 정책설정 가능, 특정 패키지에 라이선스 자동 할당 가능



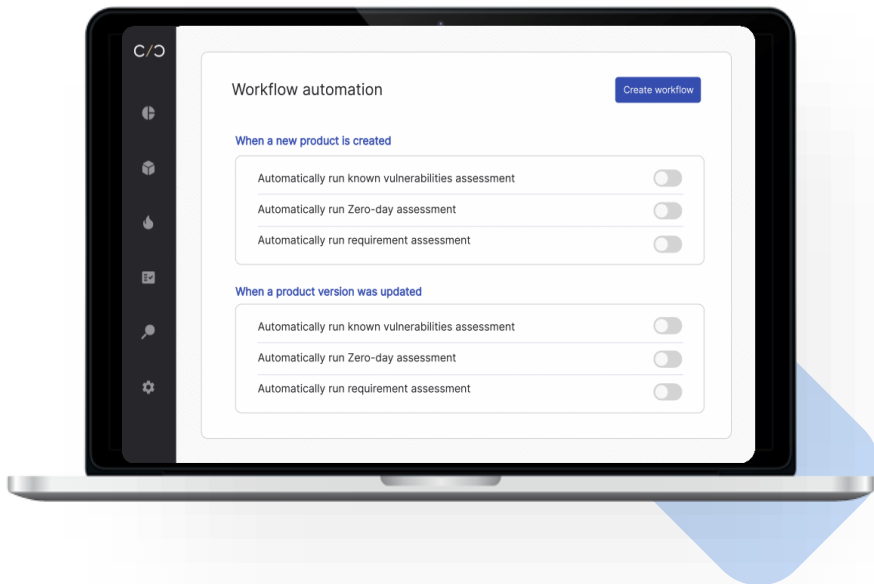
01 Cybellum 기능 – 레드팀 자동화 관리



제로데이 취약점 식별

바이너리 기반의 동적으로 검증된 엔진을 사용하여 제로데이 취약점을 식별하고
완화방안을 제공함으로써 새로운 보안 위협에
빠르게 대처할 수 있습니다.

- ▶ 오탐을 최소화, 제로데이 취약점 탐지 및 평가 등



COrporation ON by
TEChnology

CONTACT US



쿠토텍은 디지털 전환으로 대표되는 시대 변화의 흐름 속에서
안전하고 믿을 수 있는 환경을 구축하여 모두가 앞서 나갈 수 있는
세상을 만들기 위해 노력합니다.

경기도 성남시 수정구 창업로 54, 가동 609호 | 031-751-9088 | www.coontec.com

제품문의 marketing@coontec.com
제휴문의 sales@coontec.com
채용문의 hr@coontec.com

