CYTUR THREAT BRIEF | 2026년 9월

CVE 숫자만으로는 보이지 않는 선박 기자재의 실제 사이버 위험

최근 해양 기자재 Risk Assessment의 94%, 사이버 위험 완화 조치를 검토해야 하는 수준이었습니다

CYTUR

주식회사 싸이터 | www.cytur.net | info@cytur.net

발행: 2026년 9월

Prologue.
취약점의 개수보다 중요한 것은 실제 위험이었습니다

선박 기자재의 사이버보안을 이야기할 때 가장 먼저 확인하는 것은 보통 CVE입니다. 알려진 취약점이 몇 개인지, 심각도가 높은 취약점이 있는지, 최신 보안 패치가 적용되어 있는지를 봅니다. CVE는 기자재의 보안 상태를 파악하는 중요한 출발점입니다.

그런데 CVE가 많을수록 실제 사이버 위험도 반드시 높을까요?

CYTUR가 최근 수행한 10여 건의 해양 기자재 사이버 위험평가(Risk Assessment) 결과를 다시 분석해보니, 실제 현장에서는 CVE의 숫자만으로 설명되지 않는 위험이 반복적으로 확인됐습니다.

평가 대상의 **94%**가 국제선급협회(IACS) Recommendation 171 기준으로 위험 완화 조치를 적절히 고려하거나 필수적으로 검토해야 하는 **Appropriate 또는 Required** 수준으로 평가됐습니다. 평가 대상의 **약 60%**는 위험 완화 조치가 필수(Required)로 판정됐습니다.

하지만 이번 데이터에서 더 주목해야 할 부분은 따로 있습니다. 높은 위험 수준이 나타난 이유가 단순히 "CVE가 많았기 때문"은 아니었다는 점입니다.

어떤 시스템과 연결되어 있는지, 실제로 어떤 포트와 서비스가 활성화되어 있는지, 소프트웨어와 펌웨어가 어떤 상태인지, 그리고 시스템이 침해됐을 때 선박 운항에 어떤 영향을 미칠 수 있는지가 함께 위험 수준을 결정하고 있었습니다.

이번 리포트는 실제 기자재를 스캔하고 평가한 데이터를 통해 한 가지 질문에 답하려 합니다.

> **선박 기자재의 실제 사이버 위험은 무엇으로 결정되는가?**

이 질문에 답하기 위해 데이터에서 반복적으로 확인된 다섯 가지 발견을 차례로 살펴봅니다.

94%	평가 대상의 94%가 위험 완화 조치를 검토해야 하는 수준이었고, 약 60%는 조치가 필수인 Required였습니다.
10배, 같은 판정	한 시스템은 200건 이상, 다른 시스템은 20여 건의 CVE가 확인됐지만 두 시스템 모두 Required였습니다.
8개의 포트	시리얼 통신만 사용하는 기자재에서 이더넷 쪽 서비스 포트 8개가 열려 있었고, 같은 구조가 두 기자재사에서 반복됐습니다.
0건 대 13건	기자재사의 핵심 컨트롤러는 CVE 0건, 함께 설치된 네트워크 장비는 13건. 취약점은 함께 들어간 구성요소에 집중됐습니다.
20에서 12로	권고 조치와 네트워크 격리 상태를 재검증한 결과 Risk Level이 20에서 12로 낮아졌습니다. 한 사례는 3주 만에 재점검을 통과했습니다.

1. 94%가 말해주는 것

94%라는 수치를 해석할 때 먼저 짚어야 할 점이 있습니다. 이 수치는 "평가한 기자재의 94%에 취약점이 있었다"는 뜻이 아닙니다.

IACS Rec 171의 위험평가는 CVE 유무만으로 위험 수준(Risk Level)을 산정하지 않습니다. 시스템의 중요도를 나타내는 Category, 사고 발생 시 영향도(Impact), 그리고 공격 가능성을 반영한 Likelihood를 함께 고려합니다. 선박 안전에 직접 영향을 주는 중요 시스템은 이 구조 때문에 처음부터 일정 수준 이상의 Risk Level을 갖게 됩니다. 예를 들어 Category 3, Impact 4인 시스템은 Likelihood가 가장 낮은 수준이어도 "선택적 조치(Optional)" 영역으로 내려가지 않습니다.

따라서 94% 자체를 "기자재가 그만큼 취약했다"는 의미로 읽어서는 안 됩니다.

Risk Treatment	Risk Level	완화 조치의 의미
Optional	RL < 4	선택적으로 고려
Appropriate	4 ≤ RL ≤ 12	적용을 적절히 고려
Required	RL > 12	필수적으로 검토

[표 1] IACS Rec 171의 위험 처리(Risk Treatment) 기준

그럼에도 이번 결과에서 눈여겨볼 부분은 분명합니다.

Required: RL > 12 Appropriate: 4 ≤ RL ≤ 12 Optional: RL < 4
[그림 1] 위험 처리(Risk Treatment) 판정 분포, IACS Rec 171 기준 | 출처: CYTUR

시스템 중요도만으로 이 결과가 모두 정해진 것은 아닙니다. 평가 대상 사이에서 Risk Level을 가른 것은 Likelihood였고, Likelihood를 결정한 것은 네트워크 연결 구조와 활성화된 인터페이스, 서비스, 즉 실제 운용환경에서 형성된 공격표면(Attack Surface)이었습니다.

이번 데이터에서 확인하려는 핵심은 "위험이 있느냐 없느냐"가 아니라, **실제 운용환경에서 무엇이 위험을 더 높이는가**입니다.

2. CVE 는 10 배 이상 차이 났지만, 둘 다 'Required'였습니다

실제 평가 결과 가운데 주목할 만한 사례가 있습니다.

한 통합 자동화 시스템(IAS)에서는 **200건이 넘는 CVE 영향**이 확인됐습니다. 다른 통합 자동화 시스템에서는 **20여 건의 CVE**가 확인됐습니다. 확인된 CVE 수는 10배 이상 차이가 났습니다.

그런데 Risk Assessment 결과는 각각 **Risk Level 20**과 **Risk Level 16**으로, 두 시스템 모두 Required 수준이었습니다.

	시스템 A	시스템 B
확인된 CVE	200건 이상	20여 건
Risk Level	20	16
판정	Required	Required

[표 5] 두 통합 자동화 시스템(IAS)의 평가 결과 비교 | 출처: CYTUR

CVE가 적으면 위험도 그만큼 낮을 것이라고 생각하기 쉽습니다. 그러나 이 사례는 그렇지 않았습니다. CVE가 20여 건인 시스템도 200건이 넘는 시스템과 똑같이 Required였습니다.

> **CVE의 개수와 사이버 위험은 같은 지표가 아닙니다.**

CVE의 수는 알려진 기술적 취약점이 얼마나 존재하는지를 보여줍니다. 그러나 조치의 시급성과 범위는 그 취약점에 실제로 접근할 수 있는지, 다른 시스템으로 이어지는 경로가 있는지, 침해됐을 때 선박 운항에 어떤 결과를 만드는지에 따라 결정됐습니다. 중요한 것은 "몇 개의 취약점이 있는가"가 아니라 "어떤 취약점이 실제 공격 경로와 연결되는가"였습니다.

3. 위험은 CVE 목록 밖에서도 만들어지고 있었습니다

3-1. 문서상 미사용과 실제 비활성화는 다릅니다

기자재사로부터 전달받은 네트워크 구성 자료와 실제 스캔에서 확인된 활성 포트 및 서비스는 일치하지 않았습니다.

주 통신 방식이 시리얼(RS-485) 통신인 한 기자재에서는 이더넷 인터페이스가 사용되지 않는데도 **8개의 서비스 포트가 활성 상태**로 확인됐습니다. 활성 상태로 확인된 서비스의 종류는 다음과 같습니다.

확인된 서비스	기능 또는 용도
엔지니어링 통신	PLC 프로그램 업로드 및 다운로드
서버 통신	제어 명령 송수신
프린터 서비스	주 통신에 사용하지 않는 이더넷 측에서 활성 상태로 확인

[표 2] 시리얼 통신 기자재의 이더넷 측에서 확인된 활성 서비스 종류 | 출처: CYTUR

이 패턴은 한 곳에서만 나타난 것이 아니었습니다. **서로 다른 두 기자재사의 시스템에서 동일한 구조**가 확인됐습니다. 두 시스템 모두 같은 계열의 PLC와 HMI를 사용하고 있었고, 시리얼 통신만 쓰는 장비의 이더넷 측 서비스가 그대로 열려 있었습니다.

이런 서비스가 존재한다고 해서 곧바로 취약하다는 의미는 아닙니다. 하지만 필요하지 않은 포트와 서비스가 활성화되어 있다면 공격자가 접근할 수 있는 경로는 그만큼 늘어납니다. 특히 PLC 엔지니어링 포트는 비인가 프로그램 변경 시도의 통로가 될 수 있습니다.

중요한 질문은 "이 서비스가 사용되고 있는가"뿐이 아닙니다.
"사용하지 않는다면 실제로 비활성화되어 있는가"입니다.

> **사용하지 않는 문과 잠긴 문은 다릅니다.**

3-2. 취약점은 기자재 자체보다 함께 들어간 구성요소에 있었습니다

해양 기자재는 하나의 장비만으로 구성되지 않습니다. 산업용 스위치, 방화벽, 범용 운영체제, 웹 서버, 범용 PLC와 HMI 등 다양한 서드파티 구성요소가 하나의 시스템을 이룹니다.

한 평가에서는 기자재사가 직접 만든 **핵심 컨트롤러의 공개 CVE는 0건**이었습니다. 반면 함께 설치된 **산업용 네트워크 장비의 웹 관리 기능에서 13건**의 CVE가 확인됐습니다. 웹 관리 기능이 사용하는 스크립트 엔진이 구버전이었기 때문입니다.

다른 평가에서도 취약점은 범용 구성요소에서 확인됐습니다. 한 시스템에서는 함께 구성된 범용 PLC, HMI, I/O 모듈에서 **80건**, 또 다른 시스템에서는 방화벽 운영체제에서 **37건**의 CVE가 확인됐습니다.

평가 사례	구성요소	확인된 CVE
사례 A	기자재사가 직접 만든 핵심 컨트롤러	0건
사례 A	산업용 네트워크 장비의 웹 관리 기능	13건
사례 B	범용 PLC, HMI, I/O 모듈	80건
사례 C	방화벽 운영체제	37건

[표 3] 평가별 구성요소와 확인된 CVE 수 | 출처: CYTUR

이는 기자재 사이버보안을 볼 때 제품명 하나만 확인해서는 충분하지 않다는 뜻입니다. 실제로 확인해야 하는 대상은 **기자재 전체를 구성하는 하드웨어, 소프트웨어, 펌웨어의 조합**입니다. IACS UR E27이 자산 인벤토리에 하드웨어뿐 아니라 소프트웨어, 펌웨어, 인터페이스, 프로토콜 정보까지 포함하도록 요구하는 이유가 여기에 있습니다.

3-3. 권고문이 나온 지 수 년이 지난 취약점도 남아 있었습니다

또 하나 반복적으로 확인된 문제는 소프트웨어와 펌웨어의 수명주기였습니다.

공식 지원이 종료되어 더 이상 신규 보안 패치가 제공되지 않는 운영체제가 **3개 이상의 서로 다른 기자재**에서 확인됐습니다. 임베디드 Windows 계열, 모바일 운영체제 계열, 서버용 Linux 배포판 등 종류도 다양했습니다. 이 가운데 한 운영체제는 평가 시점보다 5년 전에 이미 공식 지원이 종료된 상태였습니다.

또한 **보안 권고문이 발표된 지 3년 이상 지난 취약점**이 신규 평가에서 그대로 확인되는 사례도 있었습니다. 권고문과 패치가 존재했지만, 기자재에는 반영되지 않은 채 설치된 것입니다.

선박 기자재는 한 번 설치되면 장기간 사용됩니다. 반면 소프트웨어와 펌웨어의 보안 상태는 계속 변합니다. 납품 당시에는 문제가 없었던 버전이라도 운항 기간 중 새로운 취약점이 공개될 수 있고, 납품 시점에 이미 오래된 버전이 실리는 경우도 있었습니다.

따라서 기자재 사이버보안은 납품 시점의 일회성 점검으로 끝내기 어렵습니다.

자산을 알고, 버전을 알고, 새로운 취약점과 계속 연결해서 확인해야 합니다.

4. 실제 사이버 위험을 결정한 것은 네 가지였습니다

취약점, 노출, 연결성, 영향도

이번 평가 결과를 종합하면, 실제 위험을 이해하기 위해서는 네 가지 요소를 함께 봐야 했습니다.

*아래 네 가지는 IACS Rec 171의 산식(Risk Level = 2 × (Category + Likelihood + Impact − 4))을 대체하는 것이 아니라, 산식에 들어가는 값들이 실제 기자재에서 어떻게 결정되는지를 설명하는 관점입니다. 노출과 연결성은 Likelihood를 구성하는 요소이며, 영향도는 산식의 Impact에 해당합니다.

① 취약점(Vulnerability)

알려진 CVE가 존재하는지 확인합니다. 하지만 그것만으로는 충분하지 않습니다.

② 노출(Exposure)

어떤 포트와 서비스가 실제로 활성화되어 있는지, 인증과 암호화가 적용되어 있는지 확인합니다.

③ 연결성(Connectivity)

해당 기자재가 어떤 네트워크와 연결되어 있으며, 다른 선내 시스템으로 이동할 수 있는 경로가 있는지 확인합니다.

④ 영향도(Impact)

해당 시스템이 침해됐을 때 선박의 운항, 안전, 환경에 어떤 영향을 줄 수 있는지 판단합니다.

이 네 가지를 함께 보면 CVE 목록만으로는 보이지 않던 차이가 나타납니다. 알려진 취약점이 많더라도 실제 접근 가능성이 제한되어 있다면 공격 가능성은 낮아질 수 있습니다. 반대로 CVE가 상대적으로 적더라도 원격관리 기능이 열려 있고, 다른 주요 시스템과 직접 연결되어 있으며, 해당 시스템이 선박의 핵심 기능을 담당한다면 Risk Level은 높아집니다.

취약점 스캔이 묻는 질문이 "어떤 취약점이 있는가"라면, Risk Assessment는 한 단계 더 나아가 **"그 취약점이 실제 선박에서 어떤 위험으로 이어질 수 있는가"**를 묻습니다.

5. 위험은 줄일 수 있었습니다

조치 이행과 네트워크 상태를 재검증해 위험을 재산정한 결과입니다

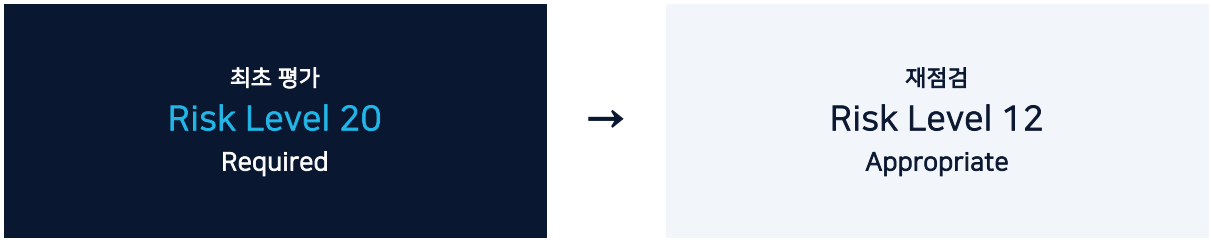
Risk Assessment의 목적은 위험을 많이 발견하는 데 있지 않습니다. 위험을 실제로 줄이는 데 있습니다.

CYTUR가 이행점검(Retest)을 수행한 한 사례에서는 최초 평가 당시 **Risk Level 20, Required**로 평가됐습니다. 이후 기자재사가 소프트웨어·펌웨어 업데이트, 불필요한 파일 전송·원격 호출 서비스 차단, 관리 인터페이스의 암호화 전환과 인증 적용 등 개선 조치를 이행했습니다.

그리고 동일한 시스템을 다시 스캔했습니다. 이 과정에서 "조치를 완료했다"는 확인서만 검토한 것이 아니라 실제 네트워크 상태를 다시 측정했습니다.

구분	조치 또는 확인 내용
개선 조치	소프트웨어와 펌웨어 업데이트, 불필요한 파일 전송 및 원격 호출 서비스 차단, 관리 인터페이스의 암호화 전환과 인증 적용
재점검	권고된 서비스 차단이 실제로 반영됐는지, 외부망과 분리된 폐쇄망에서 운용되는지, 구성이 안정화됐는지 확인
재산정	확인된 네트워크 상태를 반영해 공격표면과 Likelihood를 다시 산정

[표 4] 이행점검 사례의 조치와 검증 절차 | 출처: CYTUR



달라진 것: 권고 서비스 차단 확인 · 폐쇄망 운용 확인 · 공격표면과 Likelihood 재산정
[그림 2] 이행점검(Retest) 전후 위험 수준 변화 | 출처: CYTUR

여기서 중요한 것은 포트를 몇 개 닫았기 때문에 Risk Level이 단순히 낮아진 것이 아니라는 점입니다. 보안조치가 실제로 반영됐는지, 시스템이 어떤 네트워크 환경에서 운용되는지, 공격표면이 실제로 줄었는지를 다시 확인한 뒤 위험을 재산정했습니다.

이 사례만이 아니었습니다. 이행점검을 수행한 **복수의 사례에서 펌웨어 업데이트, 불필요 서비스 차단, 미사용 인터페이스 비활성화 등 권고 조치의 이행이 확인**됐습니다. 그중 한 사례는 **평가 보고서 발행 3주 후** 재점검에서 최초 평가에서 식별된 취약점이 모두 완화된 것으로 확인됐습니다. 정확히 무엇을 고쳐야 하는지가 특정되면, 기자재사는 빠르게 움직일 수 있었습니다.

그러나 모든 위험이 사라진 것은 아닙니다. 일부 사례에서는 서비스는 비활성화됐지만 포트가 열린 채 남았고, 다른 사례에서는 운영상 필요한 원격 화면 프로토콜이 구조적으로 평문 통신이라는 한계를 가진 채 남았습니다. 이런 항목은 외부망과 분리된 폐쇄망이라는 운용 조건을 확인하고, **잔여위험(Residual Risk)**으로 식별해 관리했습니다.

사이버보안의 목표는 위험을 무조건 0으로 만드는 것이 아닙니다.

무엇이 남아 있는지 알고, 왜 수용했는지 설명할 수 있으며, 그 상태를 계속 관리할 수 있어야 합니다.

6. 이 결과가 의미하는 것: 선주, 조선소, 기자재사에게

같은 데이터가 세 당사자에게 각각 다른 질문을 남깁니다

선주와 선박관리회사

인도받는 기자재의 CVE 개수보다 먼저 물어야 할 것은 인벤토리입니다. 하드웨어, 소프트웨어, 펌웨어 버전과 활성 포트 목록이 문서로 존재하는지, 그리고 그 문서가 실측과 일치하는지입니다. 운항 중에는 새 취약점이 계속 공개되므로, 인도 시점의 평가를 주기적으로 갱신하는 체계가 필요합니다.

- 인도 전 기자재별 자산 인벤토리(HW, SW, FW, 활성 포트) 확보
- 우선순위는 CVE 개수가 아닌 노출, 연결성, 영향도 기준으로
- 운항 단계의 정기 재평가 주기 설정

조선소

통합 단계는 설계상 격리되어 있어야 할 시스템이 실제로 격리되어 있는지 확인할 수 있는 마지막 기회입니다. 기자재사가 납품한 장비의 기본 설정, 특히 사용하지 않는 포트와 서비스가 그대로 열려 있는지는 실측으로만 확인됩니다. IACS UR E26과 E27이 요구하는 문서는 이 실측 데이터로 뒷받침될 때 설득력을 갖습니다.

- 기자재 납품 조건에 미사용 포트, 서비스 비활성화와 펌웨어 최신화 명시
- 통합, 시운전 단계에서 실측 스캔으로 설계와 실제의 차이 확인
- 조치 결과는 확인서가 아닌 재측정으로 검증

기자재사(OEM)

이번 데이터에서 취약점이 집중된 곳은 기자재사가 직접 만든 컨트롤러가 아니라 함께 넣은 스위치, 운영체제, 범용 PLC와 HMI였습니다. 자사 제품의 보안은 구매한 구성요소의 보안까지 포함합니다. 동시에 재점검 사례는 무엇을 고쳐야 하는지가 특정되면 몇 주 안에 위험 수준을 낮출 수 있다는 것도 보여줍니다.

- 자사 제품과 번들 구성요소를 포함한 소프트웨어 자산 목록(SBOM) 관리
- 출하 전 기본 설정에서 미사용 포트, 서비스, 관리 인터페이스 점검
- 조치 후 재검증 결과를 조선소, 선주에게 근거 자료로 제공

7. CVE 를 찾는 것에서 실제 위험을 관리하는 것으로

94%가 보여준 것은 단순한 취약점 통계가 아니었습니다

최근 CYTUR가 수행한 10여 건의 해양 기자재 Risk Assessment에서 94%가 위험 완화 조치를 적절히 또는 필수적으로 고려해야 하는 수준으로 평가됐습니다. 그리고 평가 대상의 약 60%는 Required 수준이었습니다.

그러나 이번 데이터가 보여준 더 중요한 사실은 따로 있습니다. 실제 위험은 CVE의 숫자 하나로 설명되지 않았습니다.

- 사용하지 않는 서비스가 열려 있었고, 같은 패턴이 서로 다른 기자재사에서 반복됐습니다.
- 주요 취약점은 기자재의 핵심 기능보다 함께 들어간 서드파티 구성요소에서 집중됐습니다.
- 지원이 종료된 운영체제와 수 년 전 공개된 취약점이 신규 평가에서 그대로 확인됐습니다.
- 그리고 정확히 무엇을 고칠지가 특정되면, 위험은 실제로 줄어들었습니다.

실제 위험을 결정한 것은 취약점, 노출 상태, 연결 구조, 시스템 영향도가 결합된 결과였습니다.

선박 기자재의 사이버보안에서 질문은 "CVE가 몇 개입니까"에서 끝나서는 안 됩니다. 그 다음 질문이 더 중요합니다.

> **"이 취약점이 실제 선박에 어떤 위험을 만들 수 있습니까?"**

CYTUR Approach

취약점 탐지에서 실제 위험 판단과 검증까지

CYTUR-SC는 실제 기자재와 선박 네트워크를 스캔해 자산, 소프트웨어와 펌웨어, 활성 포트와 서비스, 알려진 취약점을 확인합니다. CYTUR는 이 데이터를 시스템의 연결 구조와 운용환경, 영향도와 함께 분석해 IACS Rec 171 기준의 실제 사이버 위험을 평가합니다. 개선 조치 이후에는 동일한 환경을 다시 점검해 보안조치가 실제로 반영됐는지, 위험이 얼마나 감소했는지, 어떤 잔여위험이 남아 있는지를 확인합니다.

단순히 취약점을 찾는 것에서, 실제 위험을 판단하고 관리하는 것까지 CYTUR-SC.

이 리포트의 데이터에 대하여

이 리포트는 CYTUR가 최근 수행한 10여 건의 해양 기자재 단위 사이버 위험평가 결과를 IACS Recommendation 171의 동일한 위험 처리(Risk Treatment) 기준으로 재분류해 분석한 것입니다.

평가 방식

도면과 문서 검토가 아닌, CYTUR-SC 스캐너를 실제 기자재 네트워크에 연결해 자산, 펌웨어 버전, 활성 포트와 서비스, 통신 프로토콜을 실측했습니다. 식별된 자산은 공개 CVE 데이터베이스와 대조했습니다.

평가 대상

전력·추진 제어, 안전·비상정지, 자동화·통합제어, 공조, 항해·통신, 선내 IT까지 6개 카테고리에 걸친 10곳 이상 기자재사의 시스템입니다. 특정 기자재군에 한정되지 않았습니다.

위험 수준 산정

IACS Rec 171의 산식(Risk Level = 2 × (Category + Likelihood + Impact − 4))과 처리 기준(RL < 4 Optional, 4 ≤ RL ≤ 12 Appropriate, RL > 12 Required)을 적용했습니다.

표본의 한계

평가 대상은 CYTUR에 평가가 의뢰된 시스템으로, 해양 기자재 전체를 대표하는 무작위 표본은 아닙니다. 따라서 94%를 "전체 해양 기자재의 94%가 위험하다"는 의미로 해석해서는 안 됩니다. 본 리포트의 수치는 개별 기자재의 안전성 판단이 아니라, 실제 운용환경에서 반복적으로 관찰된 패턴을 설명하기 위한 것입니다.

익명성

개별 고객사, 호선, 기자재사, 제품 모델은 공개하지 않습니다.

CYTUR 소개

주식회사 싸이터(CYTUR)는 선박과 해양 기자재를 대상으로 한 사이버보안 전문기업입니다. 설계 단계의 위협모델링(TM), 건조와 인도 단계의 보안 진단(SC)과 소프트웨어 자산 목록(SBOM), 운항 단계의 침입 탐지(MG)와 위협 인텔리전스(TI)까지, 선박의 전 생애주기에 걸친 사이버 복원력을 지원합니다. CYTUR의 제품과 서비스는 ClassNK, RINA, KR 등 선급 인증을 획득했으며, 국내외 조선소와 기자재사, 선사와 함께 실제 선박 환경에서 검증되고 있습니다.

주식회사 싸이터(CYTUR)

본점: 부산광역시 해운대구 센텀중앙로 97, A-2801

서울지사: 서울특별시 금천구 벚꽃로36길 30, 가산KS타워 901호 ~ 910호

info@cytur.net | www.cytur.net

본 리포트는 CYTUR가 정보 제공 목적으로 발행한 것으로, 작성 시점에 확인된 정보와 CYTUR의 전문적 판단을 반영합니다. 해양 산업과 사이버보안 환경은 빠르게 변화하며, 발행 이후 새로운 취약점이나 위협이 나타날 수 있습니다. 본 리포트는 특정 제품이나 시스템에 대한 보안 감사 결과가 아니며 법률적, 전문적 자문으로 해석될 수 없습니다. 본 리포트의 내용을 근거로 한 의사결정과 조치의 책임은 이용자에게 있으며, CYTUR는 이로 인한 손실이나 손해에 대해 책임을 지지 않습니다. 본 리포트는 출처를 명시하는 조건으로 인용할 수 있습니다. © 2026 CYTUR Inc. All rights reserved.