

# 선박 사이버 보안 위협 모델링: VSAT 및 위성통신 취약점 분석과 대응 전략

ACK 2024

유예지, 이정연, 이지연, 양소윤, 최현우(지도교수)

2024.10.16

# 목차 페이지

## 1 서론

## 3 해운 산업의 사이버보안 위협 현황

## 5 실제 취약점 분석

Criminal IP 위협 인텔리전스 데이터 활용

주요 CVE 사례

## 7 기대 효과

## 2 VSAT 및 위성 통신 시스템 개요

## 4 연구 방법론

데이터 흐름 다이어그램(DFD) 분석

STRIDE 위협 모델링

공격 트리 분석

## 6 보안 체크리스트 강화 방안

10가지 보안 항목

사례 연구

## 8 결론 및 향후 연구

# 서론

## 배경 및 동기

- 해운 산업의 디지털화 가속으로 인한 사이버보안 위협 증가

## 연구 목적

- VSAT 및 위성 통신 시스템의 취약점 심층 분석
- 실제 사례 기반의 위협 모델링을 통한 위험 평가
- 해운 물류 산업에 특화된 보안 체크리스트를 개발

해사업계 주요 사이버 공격 사례				
시기	대상	시스템	공격유형	영향
2017	컨테이너선	선박 항해 시스템	멀웨어	10시간 동안 통제권 상실
2017	마스크	터미널 IT 시스템	랜섬웨어	3주간 시스템 마비, 3,000억 손실
2018	해운선사	회사 이메일	스피어피싱	연간 100억 규모 손실 추정
2018	COSCO 쇼핑	IT 시스템	랜섬웨어	화물 운송 지연
2018	바르셀로나 항만	항만 IT 시스템	랜섬웨어	시스템 폐쇄 및 포렌식 의뢰
2018	샌디에고 항만	항만 IT 시스템	랜섬웨어	시스템 폐쇄 및 포렌식 의뢰
2019	자동차 운반선	선박 IT 시스템	랜섬웨어	대상 시스템 포맷
2019	유조선	선박 항해 시스템	-	이란혁명수비대에 나포
2019	영국 해양업체	회사 IT 시스템	랜섬웨어	주가 하락, 포렌식 의뢰
2020	CMA CGM	회사 IT 시스템	랜섬웨어	2주간 네트워크 시스템 다운
2020	Hurghada Line	회사 IT 시스템	랜섬웨어	여권번호 등 개인정보 유출
2021	트랜스넷 SOC	항만 IT 시스템	랜섬웨어	모든 항만 터미널 운영 중단
2022	Hapag-Lloyd	회사 IT 시스템	스피어피싱	이메일 계정 통해 이메일 재전송
2022	Port of London Authority	회사 IT 시스템	분산서비스거부공격	온라인 인프라가 중단돼 오프라인으로 변환
2022	Sembcorp Marine	회사 IT 시스템	-	근로자, 운항정보에 접근

<출처: '해상 사이버 보안 동향 및 선박 사이버 안전체계 구축 방안'(한국선급, 기술정책제어연구집 2020), 해사 사이버보안 관리실무(한국선급 이카데미, 2023)>

대규모 인명 피해가 발생할 수 있는 해운업계에서의 OT 공격

피해 업체	공격	피해
컨테이너 운송 업체 덴마크 머스크라인	페트야 랜섬웨어	3주간 시스템 복구 불가 3500억원 피해



랜섬웨어가 IT 뿐 아니라 OT·ICS까지 위협하고 있음.  
사이버 보안의 필요성

# VSAT 및 위성 통신 시스템 개요

## VSAT(초소형 위성 지구국) 정의

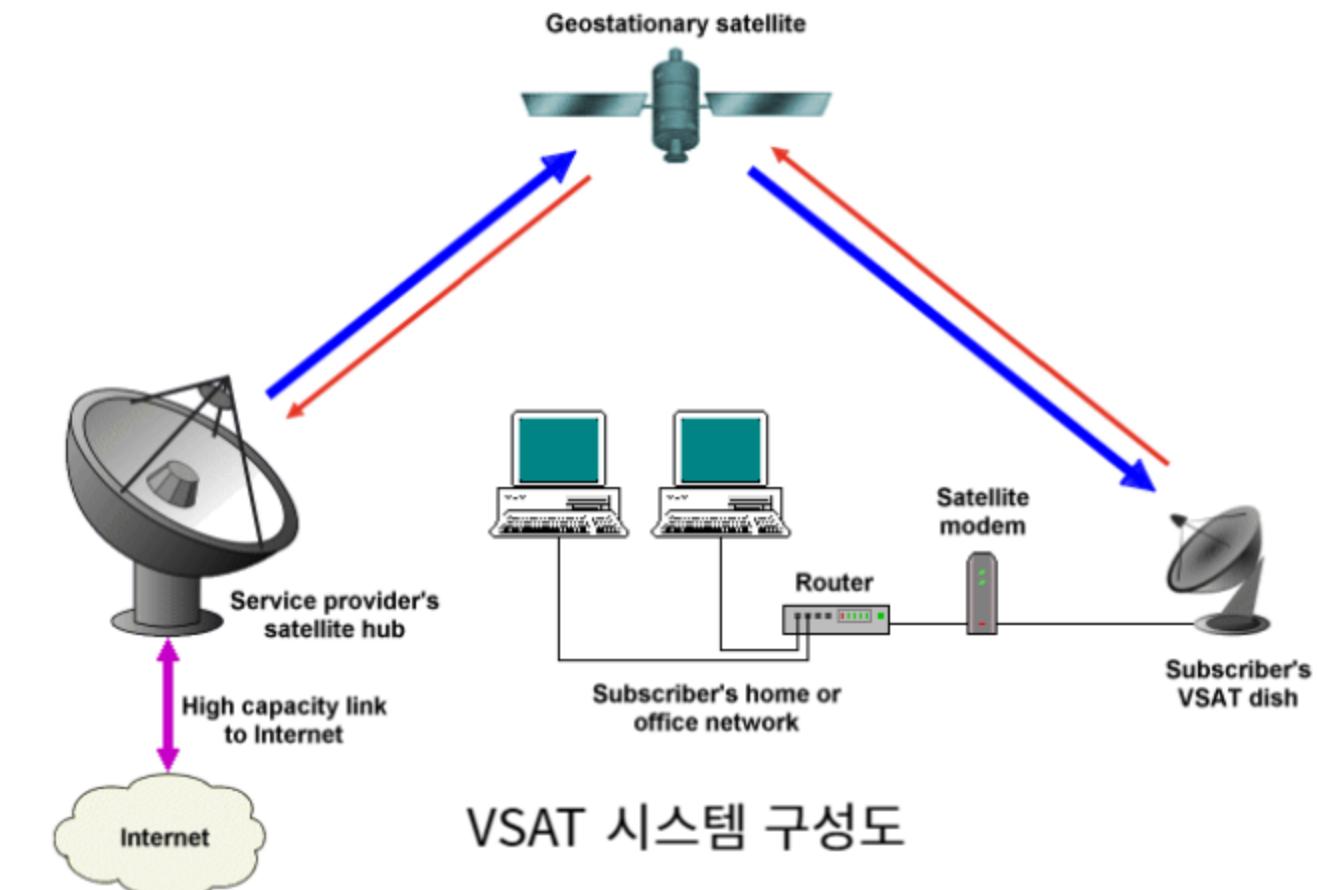
- 소형 위성 통신 시스템으로, 원거리 데이터 통신 지원
- 음성, 데이터, 영상 등 다양한 서비스 제공

## 해상 운영에서의 역할

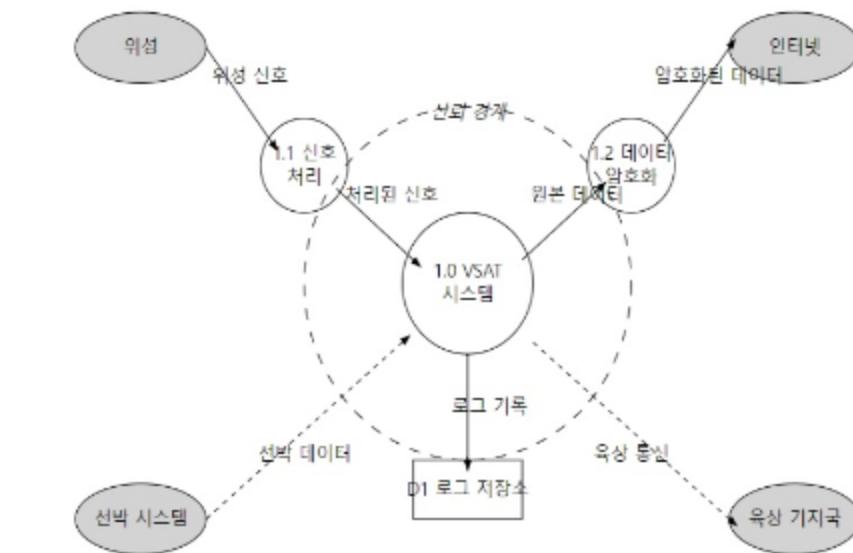
- 선박과 육상 간의 실시간 통신 연결
- 항해 데이터, 기상 정보, 화물 상태 전송
- 안전한 운항과 효율적인 해상 물류 관리 지원

## 위성 통신의 중요성

- 해양에서의 유일한 통신 수단
- 선박의 위치 추적 및 긴급 상황 대응 가능
- 해커들의 주요 표적이 됨
- 인터넷에 노출되는 것만으로도 공격 표면이 될 수 있음



VSAT 시스템 구성도



위성 통신을 통한 선박과 육상 간 데이터 흐름도

# 해운 산업의 사이버보안 위협 현황

## VSAT 시스템의 보안 취약점과 위협 증가

- 위험성: 해커가 해당 서버에 접근하여 취약점을 악용할 경우, 선박의 위성 네트워크와 연결된 다른 시스템까지 해킹 가능
- 공격 가능성: 시스템의 웹 대시보드에는 선박의 위치 정보, 장치 모델명, 버전 정보 등이 노출되어 있어, 해커가 관리자 권한을 획득하면 큰 보안 사고로 이어질 수 있음
- 여러 VSAT 시스템이 공중 인터넷을 통해 접근 가능하며, 해커가 Shodan과 같은 서비스를 통해 선박을 추적하고 기본 인증 정보로 액세스 권한을 획득할 수 있음
- 해커가 액세스 권한을 획득하면 통화 기록 확인, 시스템 설정 수정, 펌웨어 업로드 등 다양한 공격 가능
- VSAT 시스템을 통해 선박의 내부 네트워크에 접근하여 추가적인 파괴 행위 초래 가능

# 해운 산업의 사이버보안 위협 현황

## VSAT 시스템 해킹의 심각성

- 안전 위협: 선박의 위치 파악 및 실시간 추적을 통해 해적 행위나 테러에 악용 가능
- 운항 방해: 통신 중단이나 조작을 통해 선박 운항에 직접적인 영향
- 정보 유출: 항해 데이터, 화물 정보 등 기밀 정보 탈취

## 통신의 중요성과 취약성

- 해상 물류에서 통신의 핵심 역할:
  - 실시간 화물 추적, 항해 안전 관리, 기상 정보 수신 등 필수적인 기능 수행
  - 선박과 터미널을 모니터링하는 중앙집중관리 시스템 등 다양한 디지털 시스템이 통신에 의존
- 통신 장애 시 발생하는 문제:
  - 운영 지연: 스케줄 지연 및 물류 체계 혼란 초래
  - 안전 사고 위험 증가: 항해 정보 부재로 인한 충돌이나 좌초 위험
  - 재정적 손실: 운영 효율성 저하로 인한 추가 비용 발생

# 연구 방법론

데이터 흐름 다이어그램  
(DFD) 작성

- 시스템의 데이터 흐름과 취약 지점 시각화



STRIDE 위협 모델링  
적용

- 잠재적 위협 식별 및 분석



공격 트리 분석

- 공격자의 목표 달성을 위한 경로 파악



실제 취약점 데이터 수집  
및 분석

- Criminal IP 플랫폼을 통한 최신 위협 인텔리전스 활용



보안 체크리스트 개선

- 실제 사례 기반의 보안 강화 방안 제시

## 사용된 도구 및 자료

- Criminal IP 위협 인텔리전스 플랫폼
- CVE(공개 취약점) 데이터베이스
- 해운 산업 보안 보고서 및 논문

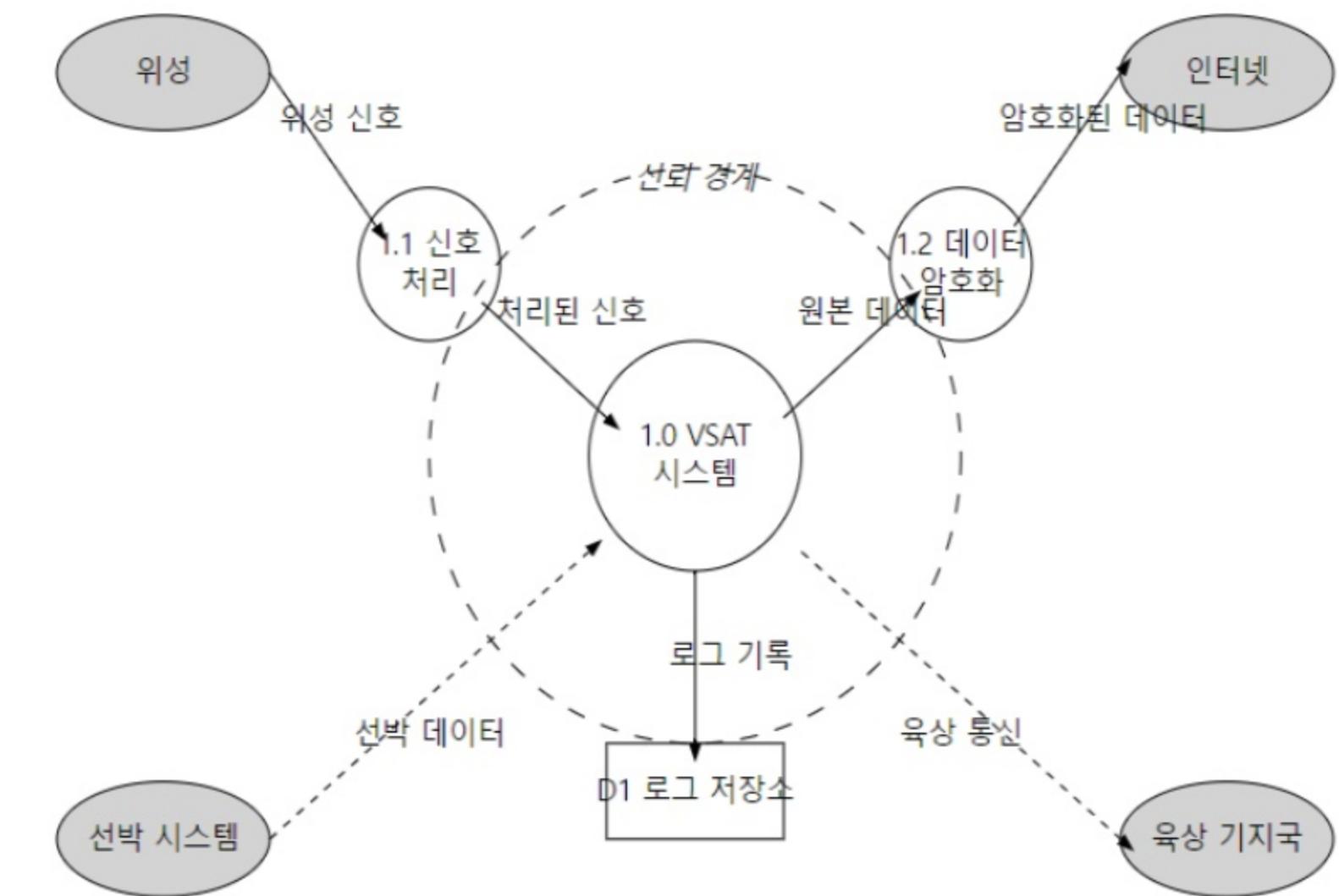
# 데이터 흐름 다이어그램(DFD) 분석

## VSAT 시스템의 DFD

- 선내 시스템 ↔ VSAT 단말기:
  - 항해 데이터, 엔진 상태 정보 전송
- VSAT 단말기 ↔ 위성:
  - 데이터 신호의 위성 전송 및 수신
- 위성 ↔ 육상 네트워크:
  - 관제 센터, 물류 시스템과의 통신

## 취약 지점 식별

- 위성 링크:
  - 신호 도청, 재밍(jamming) 가능성
- 네트워크 인터페이스:
  - 보안 프로토콜 미적용 시 외부 공격에 노출
- 데이터 저장소:
  - 암호화되지 않은 데이터의 유출 위험



위성 통신을 통한 선박과 육상 간 데이터 흐름도

# STRIDE 위협 모델링

## STRIDE 위협 모델링 개요

- STRIDE는 Microsoft에서 개발한 위협 모델링 방법론으로,  
보안 위협을 6가지 범주로 분류

위협 분류	설명	보안 속성
신원 도용 (Spoofing Identity)	타인의 계정을 이용하여 시스템 권한 획득	인증
데이터 변조 (Tempering with data)	데이터 또는 코드 변조	무결성
부인 (Repudiation)	작업 수행에 대한 부인	부인 방지
정보 유출 (Information Disclosure)	권한이 없는 사용자에게 정보 제공	기밀성
서비스 거부 (Denial of Service)	서비스 거부 또는 정상적인 서비스 제공 방해	가용성
권한 상승 (Elevation of Privilege)	권한이 없는 자가 권한을 부여받아 서비스 수행	권한 부여

STRIDE 분류

# STRIDE 위협 모델링

## 각 위협 범주 분석 및 실제 사례

공격	사례	영향
스푸핑	- 러시아 화물선이 국제 제재를 회피하기 위해 GNSS(GPS 등 위성 항법 시스템) 신호를 스푸핑하여 위치 정보를 조작.	- 선박의 실제 위치와 보고된 위치가 불일치하여 항로 이탈, 충돌 위험 증가, 국제 규제 회피 등의 문제가 발생
변조	- 2020년 일본의 나고야 항이 랜섬웨어 공격을 받아 시스템 데이터가 암호화되고 운영이 중단됨	- 해상 교통 관리 혼란, 화물 처리 지연, 안전 사고 위험 증가, 경제적 손실 발생.
부인	- 휴斯顿 항구에서 사이버 공격 발생 시, 로그 미보관으로 인해 누가 어떤 행위를 했는지 추적 불가능	- 악의적 행위 부인 가능, 책임 소재 파악 어려움, 추가적인 보안 위협 초래.
정보 공개	- 미국 해군 조선소가 랜섬웨어 공격을 받아 17,000명의 개인 정보 및 선박 설계 도면 등 기밀 정보가 유출	- 선박 위치, 화물 정보 등 민감 정보 유출로 보안 위협 증가, 국가 안보에 영향.
서비스 거부	- 2020년 국제해사기구가 DoS 공격을 받아 웹사이트 및 내부 시스템이 마비됨.	- 시스템 마비, 회원국과의 소통 중단, 경제적 손실 발생, 신뢰도 저하
권한 상승	- 해커들이 보안 통제를 우회하는 새로운 도구를 사용하여 선박 시스템의 관리자 권한을 획득	- 시스템 완전 장악, 데이터 조작 및 삭제, 악성코드 배포로 인한 추가 피해.

# 공격 트리 분석

## 공격 목표

- 선박의 항해 시스템 무력화

## 공격 경로

- 물리적 접근:
  - 내부자 또는 위장한 외부인이 직접 시스템에 접근
  - 사례: 유지보수 인력으로 가장하여 악성코드 설치
- 네트워크 기반 공격:
  - 원격 취약점 악용하여 시스템 침투
  - 사례: Maersk의 네트워크를 통한 악성코드 확산
- 사회공학적 공격:
  - 피싱 이메일을 통해 자격 증명 탈취
  - 사례: 승무원 대상 피싱 공격으로 시스템 접근 권한 획득

# 실제 취약점 분석

## Criminal IP 데이터 분석 결과

- 노출된 VSAT 장치 수: 전 세계적으로 1,627개 이상 확인
- 지역 분포: 주요 해운 국가 및 항구 주변 집중

## 주요 CVE 사례 및 영향

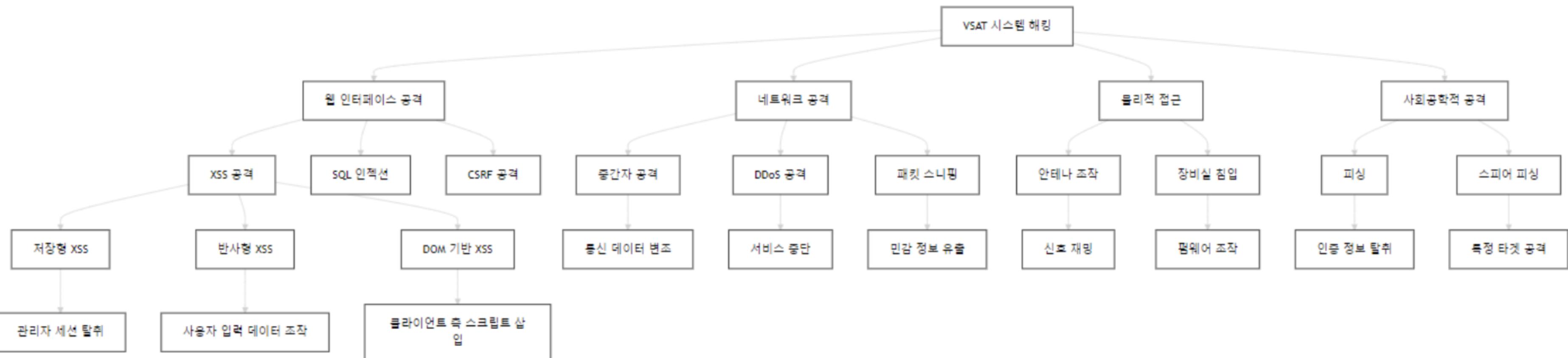
- CVE-2023-44857:
  - Cobham SAILOR VSAT 시스템의 원격 코드 실행 취약점
  - 공격자가 통신 시스템을 장악하여 데이터 유출 또는 서비스 방해 가능
  - 즉각적인 패치 적용 및 시스템 업데이트
- CVE-2022-22707:
  - 기본 자격 증명으로 인한 무단 접근 허용
  - 관리자 권한 획득으로 시스템 제어 가능
  - 기본 비밀번호 변경 및 강력한 인증 도입

운영 중단

안전 위협

재정적 손실

# 공격 트리 분석



# 보안 체크리스트 강화 방안

## DREAD 위험 평가 기법 소개

- DREAD는 보안 위협의 심각성을 평가하기 위한 방법론으로, 각 위협을 5가지 기준으로 평가
  - Damage Potential (피해 잠재력)
  - Reproducibility (재현 가능성)
  - Exploitability (공격 용이성)
  - Affected Users (영향받는 사용자 수)
  - Discoverability (발견 용이성)
- 각 기준에 대해 1~10점의 점수를 부여하고 합산하여 총점을 산출
- 총점이 높을수록 우선적으로 대응해야 할 위협

# 강화된 VSAT 보안 체크리스트

## - VSAT 시스템 펌웨어 및 소프트웨어 정기 업데이트

### STRIDE 범주

- Spoofing(S), Tampering(T), Information Disclosure(I), Elevation of Privilege(E)

### 내용 강화

- 제조사의 최신 펌웨어와 소프트웨어 패치를 주기적으로 확인하고 적용
- 자동 업데이트 기능이 있는 경우 활성화하여 보안 업데이트가 누락되지 않도록 함
- 업데이트 전에 백업을 수행하여 업데이트 실패 시 복구할 수 있도록 함

### DREAD 점수

D:9 (보안 취약점이 남아 있을 경우 심각한 피해 발생 가능)

R:8 (공격이 재현되기 쉬움)

E:7 (공격 도구가 널리 알려져 있을 수 있음)

A:9 (전체 시스템 및 사용자에게 영향)

D:6 (취약점이 공개되어 있을 가능성)

총점: 39

# 강화된 VSAT 보안 체크리스트

## - 강력한 인증 메커니즘 적용

### STRIDE 범주

- Spoofing(S), Repudiation(R), Elevation of Privilege(E)

### 내용 강화

- 비밀번호 복잡성 정책을 수립하고 최소 길이 및 문자 조합 요구사항을 설정
- 이중 인증(MFA) 또는 OTP(일회용 비밀번호) 등을 도입하여 보안 수준을 높임
- 정기적으로 비밀번호를 변경하도록 정책을 수립하고 관리자 계정을 주기적으로 점검

### DREAD 점수

D:8 (인증 정보 탈취 시 피해 발생 가능)

R:9 (공격자가 쉽게 시도하고 반복 가능)

E:8 (피싱이나 사전 공격 등으로 공격 용이)

A:9 (시스템 전체에 영향)

D:7 (인증 메커니즘의 취약점이 알려져 있을 수 있음)

총점: 41

# 강화된 VSAT 보안 체크리스트

## - VSAT 웹 인터페이스 접근 제한 및 모니터링

### STRIDE 범주

- Spoofing(S), Tampering(T), Repudiation(R), Information Disclosure(I), Elevation of Privilege(E)

### 내용 강화

- 외부에서의 직접적인 접근을 차단하고, 필요 시 VPN 등을 통해 안전하게 접근.
- 관리자 페이지의 기본 포트를 변경하고, 접근 가능한 IP 주소를 화이트리스트로 제한.
- 접근 로그를 정기적으로 모니터링하여 이상 행위를 탐지.

### DREAD 점수

D:9 (무단 접근 시 심각한 피해 가능)

R:8 (공격자가 여러 번 시도 가능)

E:8 (취약한 설정 시 공격 용이)

A:8 (중요 시스템에 영향)

D:8 (인터넷에 노출된 경우 쉽게 발견 가능)

총점: 41

# 강화된 VSAT 보안 체크리스트

## - 위성 통신 데이터 암호화 적용

### STRIDE 범주

- Tampering(T), Information Disclosure(I)

### 내용 강화

- 데이터 전송 시 SSL/TLS 등 강력한 암호화 프로토콜을 적용
- 암호화 키 관리를 철저히 하여 키 유출을 방지
- 민감한 데이터에 대해서는 추가적인 암호화(예: AES)를 적용

### DREAD 점수

D:10 (민감 정보 유출 시 심각한 피해)

R:7 (암호화되지 않은 경우 공격 재현 가능)

E:6 (암호화 우회 시도는 어려울 수 있음)

A:9 (데이터 수신자 모두 영향)

D:5 (암호화 여부는 쉽게 확인 가능)

총점: 37

# 강화된 VSAT 보안 체크리스트

## - GPS 스퓌핑 탐지 및 방어 시스템 구축

### STRIDE 범주

- Spoofing(S), Tampering(T)

### 내용 강화

- 다중 항법 시스템(GNSS) 수신기를 사용하여 신호의 무결성을 검증
- GPS 스퓌핑 탐지 솔루션을 도입하여 의심스러운 신호를 실시간으로 감지
- GPS 신호 이상 시 알림을 제공하고 수동으로 항법을 전환할 수 있는 절차를 마련

### DREAD 점수

D:10 (항로 이탈 시 안전 사고 발생 가능)

R:8 (공격자가 스퓌핑 신호 반복 송출 가능)

E:7 (스프핑 장비가 구하기 어려움)

A:10 (선박 전체에 영향)

D:6 (GPS 신호는 공개적으로 사용됨)

총점: 41

# 강화된 VSAT 보안 체크리스트

## - 네트워크 세그멘테이션을 통한 VSAT 시스템 격리

### STRIDE 범주

- Tampering(T), Information Disclosure(I), Denial of Service(D), Elevation of Privilege(E)

### 내용 강화

- VSAT 시스템을 다른 내부 네트워크와 물리적 또는 논리적으로 분리
- 방화벽과 VLAN 등을 활용하여 네트워크 간 접근을 통제
- 필요한 경우에만 최소 권한으로 네트워크 간 통신을 허용

### DREAD 점수

D:8 (격리 실패 시 피해 발생 가능)

R:7 (네트워크 구조를 파악하면 공격 가능)

E:7 (내부 네트워크 접근 시 공격 용이)

A:8 (다른 시스템에도 영향)

D:6 (네트워크 구성은 발견 어려울 수 있음)

총점: 36

# 강화된 VSAT 보안 체크리스트

## - 보안 로그 모니터링 및 이상 징후 탐지 시스템 구축

### STRIDE 범주

- Spoofing(S), Tampering(T), Repudiation(R), Information Disclosure(I), Denial of Service(D)

### 내용 강화

- 중앙 집중식 로그 관리 시스템을 도입하여 모든 로그를 수집 및 분석
- SIEM(Security Information and Event Management) 도구를 활용
- 이상 징후 탐지를 위한 규칙과 인공지능 기반 분석을 적용

### DREAD 점수

D:7 (이상 징후 미탐지 시 피해 발생 가능)

R:9 (이상 행위는 반복될 수 있음)

E:8 (공격자가 로그를 우회하려 시도 가능)

A:8 (시스템 전반에 영향)

D:9 (이상 징후는 로그로 발견 가능)

총점: 41

# 강화된 VSAT 보안 체크리스트

## - 정기적인 취약점 스캔 및 침투 테스트 수행

### STRIDE 범주

- Spoofing(S), Tampering(T), Information Disclosure(I), Denial of Service(D), Elevation of Privilege(E)

### 내용 강화

- 전문 보안업체나 내부 보안팀을 통해 정기적으로 취약점 스캔을 실시
- 실제 공격 시나리오를 기반으로 한 침투 테스트를 수행하여 보안 수준을 검증
- 발견된 취약점은 즉시 조치하고 재검증을 실시

### DREAD 점수

D:8 (취약점 미해결 시 피해 가능)

R:8 (취약점은 반복적으로 악용 가능)

E:9 (공격 도구가 널리 사용될 수 있음)

A:8 (시스템 전체에 영향)

D:9 (공개된 취약점은 쉽게 발견 가능)

총점: 42

# 강화된 VSAT 보안 체크리스트

## - VSAT 및 위성 통신 시스템 운영자 대상 보안 교육 강화

### STRIDE 범주

- Spoofing(S), Repudiation(R), Information Disclosure(I)

### 내용 강화

- 운영자들에게 최신 보안 위협과 대응 방법에 대한 정기적인 교육을 실시
- 보안 정책과 절차에 대한 숙지를 강조하고 테스트를 통해 이해도를 확인
- 사회공학적 공격(피싱 등)에 대한 대응 방법을 교육

### DREAD 점수

D:6 (인적 오류로 인한 피해 가능)

R:8 (인적 실수는 반복될 수 있음)

E:7 (공격자가 사람을 대상으로 공격 용이)

A:9 (운영자 실수는 전체 시스템에 영향)

D:8 (사람을 통한 공격은 발견 어려울 수 있음)

총점: 38

# 강화된 VSAT 보안 체크리스트

## - 사이버 보안 사고 대응 계획 수립 및 훈련

### STRIDE 범주

- Repudiation(R), Denial of Service(D)

### 내용 강화

- 보안 사고 발생 시 대응 절차를 명확히 문서화
- 정기적인 모의 훈련을 통해 대응 능력을 향상
- 사고 후 분석(Post-Incident Analysis)을 통해 개선 사항을 도출

### DREAD 점수

D:7 (신속 대응 실패 시 피해 확산)

R:9 (유사한 공격이 반복될 수 있음)

E:8 (공격자는 다양한 방법으로 공격 시도)

A:9 (시스템 전체 및 고객에 영향)

D:8 (사고 발생 시 즉시 발견 어려울 수 있음)

총점: 41

# 강화된 VSAT 보안 체크리스트

## DREAD 점수 분석 및 우선순위 결정

번호	체크리스트 항목	STRIDE	S	T	R	I	D	E	A	D	총점
1	VSAT 시스템 펌웨어 및 소프트웨어 정기 업데이트	S,T,I,E	9	9	8	9	6	7	9	6	39
2	강력한 인증 메커니즘 적용	S,R,E	8	-	9	-	8	8	9	7	41
3	VSAT 웹 인터페이스 접근 제한 및 모니터링	S,T,R,I,E	9	9	8	9	8	8	8	8	41
4	위성 통신 데이터 암호화 적용	T,I	-	10	7	10	-	6	9	5	37
5	GPS 스푸핑 탐지 및 방어 시스템 구축	S,T	10	10	8	-	-	7	10	6	41
6	네트워크 세그먼테이션을 통한 VSAT 시스템 격리	T,I,D,E	-	8	7	8	8	7	8	6	36
7	보안 로그 모니터링 및 이상 징후 탐지 시스템 구축	S,T,R,I,D	7	7	9	7	7	8	8	9	41
8	정기적인 취약점 스캔 및 침투 테스트 수행	S,T,I,D,E	8	8	8	8	8	9	8	9	42
9	VSAT 및 위성 통신 시스템 운영자 대상 보안 교육 강화	S,R,I	6	-	8	6	-	7	9	8	38
10	사이버 보안 사고 대응 계획 수립 및 훈련	R,D	-	-	9	-	7	8	9	8	41

- 정기적인 취약점 스캔 및 침투 테스트 수행 (총점: 42점)
- 강력한 인증 메커니즘 적용 (총점: 41점)
- VSAT 웹 인터페이스 접근 제한 및 모니터링 (총점: 41점)
- GPS 스푸핑 탐지 및 방어 시스템 구축 (총점: 41점)
- 사이버 보안 사고 대응 계획 수립 및 훈련 (총점: 41점)
- 보안 로그 모니터링 및 이상 징후 탐지 시스템 구축 (총점: 41점)

# 결론

## 연구 요약

- VSAT 및 위성 통신 시스템의 보안 취약점 심층 분석
- 해운 물류 산업에 특화된 강화된 보안 체크리스트 개발

## 주요 성과

- 실제 사례를 통한 STRIDE 위협 모델링 및 DREAD 위험 평가 수행
- 10개의 핵심 보안 항목을 포함한 체크리스트 제시
- 보안 체크리스트는 사이버 위협에 대한 선제적 대응 방안으로 활용 가능

# 보안 체크리스트의 활용 및 기대 효과

## 활용 방안

- 선박 운영자 및 해운 기업에서의 보안 정책 수립 시 참고 자료로 활용
- VSAT 시스템 구축 및 운영 시 보안 강화 지침으로 적용
- 보안 감사 및 평가 시 체크리스트를 활용하여 취약점 점검

## 주요 성과

- 사이버 공격으로 인한 운영 중단 및 재정적 손실 감소
- 선박 및 화물의 안전성 향상으로 신뢰도 제고
- 국제 보안 표준 및 규제 준수를 통한 경쟁력 강화

# 향후 연구 방향

## 보안 체크리스트의 확대 및 보완

- 추가적인 보안 항목 발굴 및 업데이트를 통한 체크리스트 완성도 향상
- 다양한 선박 유형 및 해운 시스템에 적용 가능한 범용 체크리스트 개발

## 자동화된 보안 점검 도구 개발

- 체크리스트 기반의 자동화된 취약점 스캐닝 및 진단 도구 연구
- 인공지능 및 머신러닝을 활용한 이상 행위 탐지 시스템 개발

## 산업 협력 및 표준화 노력

- 해운 기업, 보안업체, 정부 기관과의 협력을 통한 보안 솔루션 실용화
- 국제 표준 기구와의 협력을 통한 보안 체크리스트의 표준화 추진

감사합니다