

항공우주

하늘을 지키는 기술

세계 유수의 공항 및 항공 기관에서
신뢰하는 전문 사이버 보안 솔루션

LRQA



목차



소개 – 오늘날 항공 산업은 전례 없는 사이버 보안 위험에 직면해 있습니다

03 >

중요 항공 운영에서 사이버 보안 성숙도 강화

04 >

LRQA 개요

05 >

사이버 보안 솔루션

06 >

거버넌스, 위험 및 규정 준수

06 >

보안 테스트

07 >

사이버 보안 권고

08 >

관리형 사이버 보안 서비스

09 >

사고 대응

10 >

왜 LRQA인가?

11 >

오늘날의 항공 산업은 전례 없는 사이버 보안 위험에 직면해 있습니다.



디지털 시스템, 상호 연결된 인프라 및 타사 공급업체에 대한 의존도가 높아짐에 따라 항공 산업이 직면한 사이버 위협의 규모와 정교함이 계속 증가하고 있습니다. 지난 12개월 동안 항공 관련 조직의 55%가 랜섬웨어 공격을 경험했으며, 이로 인해 운영 중단과 데이터 손실이 발생했습니다 (**Bridewell 보고서**). 또한, **SysDream**에 따르면 2024년 한 해 동안 항공 분야에서는 총 604건의 사이버 공격이 문서화되었으며, 이 중 대부분은 DDoS(분산 서비스 거부) 공격이었습니다.

공항, 항공사, 항공기 제조사는 이제 랜섬웨어 조직, 국가 차원의 해커, 범죄 네트워크의 주요 표적이 되고 있으며, 이는 안전, 서비스 연속성, 규제 준수에 실질적인 위협을 초래하고 있습니다.

이제 조직은 인프라 수준의 보호, 항공 산업에 특화된 인사이트, 그리고 글로벌 인증 경험을 제공하는 신뢰할 수 있는 공인 파트너가 절실히 필요합니다.

84+

LRQA는 전 세계 84개 이상의 공항과 신뢰를 바탕으로 파트너십을 맺고 있으며, 2024년 한 해에만 17,000일 이상의 세계적 수준의 침투 테스트 서비스를 제공했습니다.

중요한 항공 운영에서 사이버 보안 성숙도 강화

LRQA의 전담 사이버 보안 전문팀은 항공 산업 생태계 내 사이버 리스크의 현실을 깊이 이해하고 있습니다. 이는 우리가 해당 산업의 핵심에서 활동하는 조직들과 지속적으로 협력해 오고 있기 때문입니다. 당사는:

CBEST, TIBER-EU, GBEST와 같은 프레임워크에 따라 사이버 보안 테스트 및 인텔리전스 서비스를 제공할 수 있는 공인 기관입니다

복잡하고 규제가 엄격한 환경에서 IT 및 OT 시스템 전반에 걸쳐 사이버 보안 보증 서비스를 제공한 풍부한 경험을 보유하고 있습니다

OT, 에어사이드 시스템, 티켓팅 플랫폼, SCADA 등 다양한 분야에서 경험을 갖춘 CTC, SC 및 DV 등급 자격 보유 컨설턴트로 구성되어 있습니다

보잉 에어로스트럭처스, GE 애비에이션, GKN 에어로스페이스, 탈레스 아비오닉스, 스위스포트 ATM, 콩스버그 애비에이션 메인테넌스를 비롯한 항공 공급망 내 주요 OEM을 포함한 세계적인 수준의 항공사에 대해 승인된 심사 및 자문을 수행하고 있습니다

침투 테스트, 위협 인텔리전스, 사고 대응, 레드팀 운영, 보안 관제(SOC) 서비스 전 분야에서 CREST의 전 영역 인증을 보유한 전 세계 유일의 공급업체입니다



LRQA 란?



전 세계

84

개 이상의 공항에서
신뢰를 받고 있습니다.

250+

글로벌 사이버 보안
전문가, 주요 항공
고객과 협력

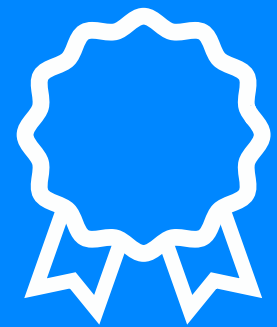


전체 CREST
인증을 받은
전 세계 유일의
제공업체



#1

보안 운영 센터
서비스에 대한 최초의
CREST 인증 획득



수상

올해의 보안 공급업체(Security Vendor
of the Year), 최고의 침투 테스트 서비스 등
(Best Penetration Testing Service) 수상

1000+

항공 및 항공우주 설계, 생산 및 MRO
조직이 AS 91XX 표준에 인증됨

84+

CAA ASSURE에서 ISO 27001 정보
관리 시스템 보안을 포함한 ISO 표준에
이르기까지 전 세계 84+ 공항 지원

[LRQA의 사이버 보안 서비스에 대해 자세히 알아보기](#)

거버넌스, 리스크 규정 준수

항공 사이버보안 규제에 대한 준수를 달성하고 장기적인 복원력을 구축하세요.

오늘날의 글로벌 항공 환경에서 조직은 데이터 프라이버시 법부터 항공 산업 특화 사이버보안 규제 및 프레임워크에 이르기까지 빠르게 변화하는 규제 환경을 효과적으로 관리해야 합니다. 공항, 항공사, 운행사, 제조사, 항공교통서비스제공자(ANSP), 그리고 그 외 공급망 전반은 민감한 운영 정보와 승객 데이터를 어떻게 관리, 저장 및 보호하는지에 대해 엄격한 감시를 받고 있으며, 그에 따른 리스크는 매우 큼니다.

GDPR, NIS2, DORA, PCI DSS 등의 규제를 위반할 경우 수백억 원에 달하는 벌금이 부과될 수 있습니다. 특히 항공처럼 안전이 최우선이며 신뢰가 중요한 산업에서는, 규제 불이행으로 인한 평판 훼손이 금전적 손실보다 더 오랜 기간 영향을 미칠 수 있습니다.

당사의 전문가들은 다음과 같은 분야에서 귀사를 지원할 수 있습니다:

- 사이버 보안 거버넌스를 국내외 법률에 선제적으로 조정
- 규제 요건을 충족하고 이를 초과하는 정책 및 절차 수립
- 복잡한 글로벌 운영 및 제3자 네트워크 전반의 규제 준수 보장
- 사전 점검, 갭 분석 및 자문 지원을 통해 리스크 완화

솔루션

ISO 27001

정보 보안 경영

NIS2 지침

네트워크 및 정보 보안 요구 사항

NIST 사이버 보안 프레임워크(CSF)

CAF

NCSC 사이버 평가 프레임워크

CAA ASSURE

UK Civil Aviation Authority의
사이버 보안 감사 프레임워크

GDPR

일반 데이터 보호 규정(General
Data Protection Regulation)

DORA

디지털 운영 복원력법(Digital
Operational Resilience Act)
(항공 금융/IT 서비스)

PCI DSS

결제 카드 산업 데이터 보안 표준

LRQA의 거버넌스, 리스크 및 컴플라이언스 서비스

보안 테스트

취약점을 식별하고, 사이버 리스크를 줄이며, 실제 시나리오 기반의 테스트를 통해 방어 체계를 검증하세요.

오늘날 항공 운항이 직면한 사이버 위협을 이해하려면, 조직은 공격자의 관점에서 사고해야 합니다. LRQA의 보안 테스트 서비스는 실제 사이버 위협을 시뮬레이션하도록 설계되어 있으며, 정보기술(IT)과 운영기술(OT) 전반에 걸쳐 취약점을 식별하고, 이를 악용당하기 전에 사전에 대응할 수 있도록 지원합니다. 이를 통해 가장 중요한 영역에서 회복력을 구축할 수 있습니다.

CREST 인증 테스터들로 구성된 팀이 깊이 있는 기술 지식과 사람 중심의 평가 방식을 활용하여 조직의 인프라, 애플리케이션, 그리고 에어사이드(공항 측) 시스템 전반의 방어 체계를 평가합니다. 귀사의 기술, 프로세스, 위협 프로필에 맞추어 테스트를 설계하여, 실질적이고 항공 산업에 부합하는 결과를 보장합니다.

LRQA의 사이버 보안 전문가들은 다음과 같은 지원을 제공합니다:

- 디지털, 운영, 클라우드 인프라 전반에 걸쳐 숨겨진 취약점을 식별합니다
- 공격자가 항공 산업 특유의 시스템과 도메인에서 어떤 방식으로 취약점을 악용할 수 있는지 파악합니다
- 현실적인 위협 시나리오 하에서 탐지, 보고, 대응 역량을 평가하고, 관련 규제 보고 메커니즘과의 정합성을 확인합니다
- 명확하고 리스크 기반의 평가와 조치 방안을 통해 보완 조치의 우선순위를 설정할 수 있도록 지원합니다

솔루션

침투 테스트

모든 항공 기능 영역에 걸쳐 네트워크, 장치, 프로세스 및 인력에 대한 실제 테스트

웹 애플리케이션 테스트

특히 OSS 패키지에서 애플리케이션 수준 위험을 식별하고 해결합니다.

클라우드 침투 테스트

IT 및 OT 패키지를 호스팅하는 클라우드 환경(AWS, Azure, GCP)에 대한 공격 시뮬레이션

모바일 애플리케이션 테스트

모바일 OT 및 자산 전반에서 사용자 및 운영 데이터를 보호하기 위한 iOS 및 Android 평가

레드 팀

지속적이고 정교한 공격 경로에 대한 은밀한 시뮬레이션

사회공학 엔지니어링

인적 및 절차적 취약성으로 인한 위험 식별

버그 바운티 플랫폼

지속적인 위협 헌팅을 위해 검증된 연구원으로 구성된 선별된 커뮤니티에 액세스

지속적인 보증

공격 표면 관리 및 시나리오 테스트를 통한 지속적인 위험 가시성 확보

Purple Teaming

탐지 및 대응 역량 강화를 위한 협업 테스트

LRQA의 보안 테스트 서비스

사이버 보안 어드바이저리

위협을 이해하고 회복탄력성을 강화하며 사이버 보안 성숙도를 높이기 위한 전략적 가이드

항공 산업은 시스템 간 상호 연결성이 높고 안전에 직결되기 때문에, 사이버 위협에 단순히 대응하는 것만으로는 충분하지 않습니다. 조직은 운영 환경과 위협 환경의 변화에 발맞춰 진화할 수 있는 전략적이고 인텔리전스 기반의 접근 방식으로 리스크를 식별하고 완화해야 합니다.

LRQA의 사이버 보안 어드바이저리 서비스는 귀사의 현재 보안 성숙도를 평가하고, 가장 큰 리스크가 어디에 있는지 파악하며, 조직의 리스크 수용 범위와 규제 요건에 적합한 통제를 도입할 수 있도록 지원합니다.

당사의 전문가는 다음과 같은 방식으로 귀사를 지원할 수 있습니다:

- 디지털 리스크 프로파일과 위협 환경에 대한 가시성을 확보
- 운영, 인프라 및 고객 신뢰를 보호하기 위한 맞춤형 사이버 전략 수립
- 보안 성숙도와 리스크에 기반하여 투자 우선순위 결정
- 전략적 로드맵, 통제 방안 및 교육을 통해 회복력과 대응 역량 강화

솔루션

사이버 보안 성숙도 평가

인력, 프로세스 및 기술 전반의 격차를 파악하고 개선 우선순위를 정합니다.

위협 인텔리전스 서비스

진화하는 항공 에코시스템 사이버 위협에 앞서 나갈 수 있는 실행 가능한 인사이트를 제공합니다.

가상 CISO(vCISO)

정규직 고용 비용 없이 고위급 사이버 리더십에 액세스

인수합병 실사

거래 전 대상 기업의 사이버 리스크 평가

위협 감시시스템

지속적인 공격 표면 모니터링을 통해 관리형 사이버 위협 인텔리전스

위협 모델링

잠재적인 공격 경로를 매핑하여 중요한 항공 시스템 및 자산을 더 잘 보호할 수 있습니다.

규정 준수 권고

GBEST(UK Cabinet Office), CBEST(UK Bank of England), TIBER-EU(EU 테스트 프레임워크), U.S. NIST(National Institute of Standards and Technology), PCI DSS(Payment Card Industry Data Security Standard) 및 CMMC(미국 국방부의 민감한 데이터 처리)와 같은 IT 보안 프레임워크를 구현하려는 조직을 위한 것입니다.

공격적 보안 교육

내부 팀에 실무 기술을 제공하여 방어를 개선합니다.

LRQA의 사이버 보안 자문 서비스

관리형 사이버 보안 서비스

항공 운영에 최적화된 24시간 맞춤형 사이버 방어 솔루션으로 보안 역량을 강화하세요.

항상 가동되어야 하고, 안전과 규제 신뢰가 필수인 항공 산업에서는 범용 보안 툴만으로는 충분하지 않습니다. 실시간으로 위협을 모니터링하고, 사고에 즉각 대응하며, 보안 운영을 비즈니스 전략과 정렬시킬 수 있는 신뢰할 수 있는 파트너가 필요합니다.

LRQA의 사이버 보안 매니지드 서비스는 글로벌 보안 관제 센터(SOC)와 사이버 사고 대응팀(CIRT)을 통해 24시간 위협 감지, 사고 대응, 보안 보증을 제공합니다. 복잡한 사이버 리스크 관리를 단순화하고, 내부 부담 없이 조직의 보안 성숙도를 강화할 수 있도록 지원합니다.

당사의 전문가들은 다음을 지원해드립니다:

- 사이버 위협을 실시간으로 탐지, 조사 및 대응
- 선제적이고 확장 가능한 방어 체계를 통해 사이버 복원력 강화
- IT 및 OT 환경 전반의 취약점을 모니터링하고 관리
- 항공 산업 특유의 리스크와 규제 준수 요구사항에 맞춰 관리형 서비스를 조정

솔루션

관리 위협 및 규정 준수

- 컨설팅 및 규정 준수 평가
- 가상 CISO(vCISO) 서비스
- 사이버 위협 평가
- 위협 워크숍 및 위협 모델링

관리형 방어 서비스

- 관리형 탐지 및 대응(MDR)
- 확장된 탐지 및 대응(XDR)
- 침해 사고 대응 및 디지털 포렌식
- 취약성 관리

관리형 보안 보증

- 침투 테스트
- 지속적인 위협 노출 관리
- 레드 팀 구성
- 클라우드 보안 평가

LRQA의 관리형 사이버 보안 서비스

인시던트 대응

사이버 사고의 영향을 최소화하고, 전문가 주도의 조사, 차단 및 복구를 통해 더 빠르게 회복하세요.

항공 산업에서는 사이버 사고가 빠르게 확산되어 운영 중단, 서비스 마비, 규제 위반 등으로 이어질 수 있습니다. 랜섬웨어 공격, 데이터 유출, 핵심 시스템의 침해 등 어떤 사고든 빠르고 효과적인 대응은 인명 보호, 자산 보호, 평판 유지를 위해 매우 중요합니다.

LRQA의 인시던트 대응 서비스는 사고에 대한 사전 준비부터 대응, 복구까지 고객이 신뢰를 가지고 수행할 수 있도록 설계되었습니다. LRQA의 글로벌 사이버 사고 대응팀(CIRT)은 고객 조직과 긴밀히 협력하여 위협을 차단하고, 사고의 근본 원인을 조사하며, 항공 산업의 규제 요건을 준수하면서 복구 및 이해관계자 신뢰 확보를 지원합니다.

당사의 사이버 보안 전문가들은 다음과 같은 지원을 제공합니다:

- 실시간 사이버 사고에 신속하고 효과적으로 대응
- 운영 및 평판에 미치는 영향을 최소화하기 위한 위협 차단
- 사고의 근본 원인 분석 및 디지털 포렌식 조사 지원
- 시나리오 기반 대응 매뉴얼, 모의 훈련, 사전 계획 수립을 통한 내부 대응 역량 강화

솔루션

비상 사고 대응

활성 위협을 억제하고 완화하기 위한 24/7 지원

사이버 사고 대응 플레이북

운영에 맞게 조정된 맞춤형 역할별 지침

사고 대비 평가

준비 및 대응 역량 평가

디지털 포렌식 및 조사

사고 방식, 시기 및 위치 파악

모의 연습

실제 시나리오를 시뮬레이션하여 내부 반응을 테스트합니다.

인시던트 후 검토

공격으로부터 배우고 방어를 강화합니다.

LRQA의 사고 대응 서비스

왜 LRQA와 함께해야 할까요?

당사는 항공 산업의 조직들이 고유한 사이버 보안 과제에 직면해 있다는 것을 잘 알고 있습니다. 이는 운영 기술과 에어사이드 인프라 보호부터 승객 데이터 보안, 글로벌 규제 준수에 이르기까지 다양합니다.

LRQA의 경험에 따르면 이러한 과제는 대규모이면서 기술적으로 복잡한 프로그램을 요구하는 경우가 많으며, 이는 여러 사이트, 레거시 시스템, 그리고 중단 없는 운영 요건을 포함합니다. 이러한 환경을 안전하고 효율적으로 관리하려면, 기술적 깊이와 항공 산업에 대한 전문성을 모두 갖춘 파트너가 필요합니다.

당사의 전문성을 통해 귀사는 다음과 같은 이점을 얻을 수 있습니다:

- ✓ 조직 전체 자산에 대한 취약점 통합 뷰 제공
- ✓ 의사결정을 위한 포괄적인 분석
- ✓ 데이터 시각화 기능
- ✓ 컨설턴트 및 프로그램 팀과의 실시간 협업
- ✓ 결과 및 개선 조치에 대한 접근
- ✓ 스케줄링 시간 단축

LRQA의 사이버 보안 서비스에 대해 자세히 알아보기

LRQA의 차별점은 무엇인가요?

- 허니트랩부터 보안 운영센터(SOC) 성숙도 모델에 이르기까지, 독자적인 도구와 기술을 개발하는 전담 연구·혁신팀 보유
- 복잡한 항공 운영 환경에도 유연하게 적용 가능한 전문 서비스 및 매니지드 서비스 포트폴리오
- 독자적인 툴링을 통해 일부 테스트를 자동화하여, 컨설턴트가 고도화된 위협 대응에 집중할 수 있도록 지원
- 실제 시스템에서 제로데이 취약점을 발견하고, 이를 통해 글로벌 위협 인텔리전스에 기여
- 전 세계 유일하게 모든 CREST 공인 분야(침투 테스트, 위협 인텔리전스, 사고 대응, 레드팀 운영, SOC 서비스) 인증 보유



84+

전 세계 84 여개 공항을 대상으로 CAA ASSURE부터 ISO 표준(ISO 27001 정보보안경영시스템 등)까지 지원합니다.

1000+

항공 및 우주 산업의 설계, 생산, 정비 (MRO) 조직은 AS 91XX 표준에 따라 인증을 받습니다

17,000+

2024년 한 해 동안 17,000 일 이상의 침투 테스트를 수행했습니다

250+

250명 이상의 전담 사이버 보안 전문가 보유

“LRQA는 우리에게 대해, 우리의 운영 방식과 우리가 달성하고자 하는 목표에 대해 진심으로 이해하려고 노력하는 것이 느껴졌습니다. 우리는 새로운 관점을 제시하고, 우리에게 도전 의식을 줄 수 있는 파트너와 함께 일하고 싶었습니다.”

- 버밍엄 공항 -



LRQA 소개

LRQA는 선도적인 글로벌 보증 파트너로, 평가, 자문, 검사 및 사이버 보안 서비스에 대한 수십 년의 타의 추종을 불허하는 전문성을 결합합니다.

저희의 솔루션 기반 파트너십은 고객이 가장 큰 비즈니스 과제를 해결하는 데 도움이 되는 데이터 기반 통찰력으로 지원됩니다. 150개국 이상에서 운영되며 5,000명 이상의 팀을 보유한 LRQA의 수상 경력이 있는 규정 준수, 공급망, 사이버 보안 및 ESG 전문가 61,000개 이상의 고객이 그들이 운영하는 곳 어디에서나 위험을 예상, 완화 및 관리하도록 돕습니다.

모든 업무에서 우리는 우리의 사람들, 고객, 지역사회 및 지구를 위한 더 나은 미래를 형성하기 위해 최선을 다하고 있습니다.

문의

더 자세한 정보는 홈페이지(lrqa.com/ko-kr)를 방문하거나, 전화(+82 2 736 6231)로 문의해 주시기 바랍니다.



LRQA
2F T Tower
30 Sowol-ro 2-gil
Jung-gu, Seoul
Republic of Korea
04637

모든 정보가 정확하고 최신 상태로 유지되도록 주의를 기울이고 있습니다. 그러나 LRQA는 정보의 부정확성이나 변경에 대해 책임을 지지 않습니다.