SAMRIDDHI Volume 13, Issue 2, 2021 Print ISSN: 2229-7111 Online ISSN: 2454-5767

DevSecOps Integration in Cruise Industry Systems: A Framework for Reducing Cybersecurity Incidents

Suresh Vethachalam*

Centene Corporation, St Louis, USA.

Abstract

The cruise industry has undergone significant digital transformation, integrating advanced IT and operational technologies to enhance navigation, onboard services, passenger experiences, and operational efficiency. However, this rapid evolution has simultaneously expanded the cybersecurity attack surface, exposing cruise lines to increasingly sophisticated threats such as ransomware, data breaches, and system intrusions. Traditional security approaches, which often treat cybersecurity as a final-stage concern, have proven inadequate for protecting the dynamic and distributed architectures typical of maritime systems.

This article presents a tailored DevSecOps framework designed to embed security early and continuously throughout the software development lifecycle in cruise industry systems. By aligning continuous integration/continuous delivery (CI/CD) practices with automated security testing, infrastructure as code, and runtime threat detection, the proposed approach enables a proactive and resilient security posture. Drawing on principles of risk-based prioritization and shift-left security, the framework addresses the unique constraints of maritime operations, including intermittent connectivity, hybrid legacy systems, and regulatory compliance. The paper also outlines implementation strategies, evaluates hypothetical use cases, and identifies measurable benefits such as reduced mean time to remediation (MTTR), improved vulnerability management, and enhanced regulatory readiness. Ultimately, it argues for a paradigm shift in how cruise operators, vendors, and regulators approach cybersecurity moving from reactive containment to integrated, preventive defense through DevSecOps.

Keywords: DevSecOps, Cruise Industry, Maritime Cybersecurity, Secure Software Development, Operational Technology (OT) Security.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2021); DOI: 10.18090/samriddhi.v13i02.15

Introduction

The cruise industry has become increasingly reliant on complex digital infrastructures to deliver seamless operations and high-quality passenger experiences. From shipboard automation and navigation systems to passenger Wi-Fi, cloud-based booking engines, and data-driven logistics, cruise lines have embraced digital transformation as a competitive imperative. This convergence of operational technology (OT) and information technology (IT) has created highly interconnected ecosystems that, while enhancing service delivery, also introduce significant cybersecurity vulnerabilities.

High-profile cyber incidents targeting maritime assets have underscored the urgent need for more robust security strategies. Legacy systems, limited onboard IT staff, third-party software dependencies, and satellite-based connectivity further complicate threat mitigation in cruise environments. Traditional security models where protections are bolted on after development or rely heavily on perimeter defense are insufficient for securing the continuous deployment pipelines and distributed architectures that now characterize modern cruise operations.

DevSecOps offers a promising solution. By embedding security as a core component of the software development lifecycle, DevSecOps integrates security practices into every phase of development, from planning to deployment and monitoring. It emphasizes automation, collaboration,

Corresponding Author: Suresh Vethachalam, Centene Corporation, St Louis, USA, e-mail: suresh.vedha@gmail.com

How to cite this article: Vethachalam, S. (2021). DevSecOps Integration in Cruise Industry Systems: A Framework for Reducing Cybersecurity Incidents. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 13(2), 158-167.

Source of support: Nil

Conflict of interest: None

continuous testing, and "shift-left" strategies that detect and remediate vulnerabilities early before they propagate into production.

This article explores how DevSecOps can be effectively adapted to the cruise industry's unique operational context. It outlines a tailored implementation framework, discusses practical case scenarios, and identifies critical success factors. By doing so, the article contributes to both industry practice and the broader cybersecurity discourse by advocating for an integrated, preventive approach to digital risk in maritime environments.

The Evolving Threat Landscape in Maritime and Cruise Sectors

As maritime industries increasingly rely on integrated digital ecosystems, the cruise sector has emerged as a significant target for cyber threats. Once dependent solely on mechanical systems, modern cruise operations now rely on complex digital infrastructures including cloud-based booking platforms, shipboard operational technologies (OT), and networked passenger services. This digital transformation, while enhancing efficiency and user experience, has also expanded the attack surface for malicious actors. Understanding the nature, scale, and vectors of these cybersecurity risks is essential for designing robust frameworks such as DevSecOps that can preemptively embed security throughout system lifecycles.

Increased Connectivity and Attack Surfaces

Modern cruise ships operate as floating smart cities, equipped with thousands of connected devices and systems, ranging from engine control units to passenger Wi-Fi networks. The convergence of IT (Information Technology) and OT (Operational Technology) onboard these vessels has created a hyper-connected environment susceptible to both targeted and opportunistic cyberattacks. Systems such as GPS, automated navigation, propulsion, HVAC, and crew communications are increasingly software-defined, making them vulnerable to tampering, malware propagation, and denial-of-service (DoS) attacks. Furthermore, the growing reliance on satellite communications for real-time data transfer introduces additional vulnerabilities due to bandwidth limitations and encryption challenges.

Prominent Threat Vectors

Cyber threats in the cruise industry manifest through a range of attack vectors. Phishing remains a predominant entry point, often targeting crew members and administrative staff through email spoofing and credential theft. Insider threats, whether intentional or accidental, also pose considerable risk particularly in environments where access controls and identity management are not rigorously enforced. In addition, third-party vendors that provide IT services, maintenance, or cloud-based applications often lack standardized security protocols, thereby becoming a weak link in the digital supply chain. The deployment of insecure APIs and outdated software patches further compounds these risks, leaving ships exposed during critical voyage periods.

Implications for Safety, Privacy, and Compliance

The ramifications of cyber incidents extend beyond financial or reputational damage. In maritime contexts, successful cyber intrusions can compromise navigational accuracy, disable propulsion systems, or trigger false alarms posing direct threats to crew and passenger safety. Furthermore, cruise operators collect and process vast volumes of personal and financial data through their digital platforms. A breach in these systems can result in widespread data leaks, identity theft, and legal liability. Regulatory frameworks such as the International Maritime Organization's (IMO) cybersecurity guidelines and regional data protection laws increasingly hold operators accountable for cybersecurity lapses. However, compliance alone does not equate to resilience; proactive integration of security into development and operations remains crucial.

The Need for a Paradigm Shift

Traditional perimeter-based security approaches are no longer sufficient in this evolving threat landscape. The dynamic and mobile nature of cruise ship systems requires adaptive, continuous security measures that can scale with operational demands. Emerging threat intelligence reports increasingly highlight the need for integrating security from the outset of system design emphasizing continuous monitoring, automated testing, and collaborative incident response protocols. This context provides a compelling rationale for the adoption of DevSecOps methodologies in the cruise sector, where speed, scale, and security must be tightly aligned.

In sum, the maritime and cruise industries are undergoing a digital evolution that, while offering substantial operational benefits, introduces a multifaceted cybersecurity threat landscape. Increased connectivity, evolving threat vectors, and stringent compliance demands necessitate a more agile and integrated security framework. Understanding these challenges is foundational to the strategic adoption of DevSecOps, which offers a path forward by embedding security practices into the entire system development and deployment pipeline. The next section will explore the core principles of DevSecOps and how they address these emerging cybersecurity risks.

Principles and Practices of DevSecOps

The integration of security into agile software delivery pipelines has gained prominence as organizations contend with evolving threat vectors and increasingly complex digital infrastructures. In maritime technology systems, such as those used by cruise operators, traditional perimeter-based security approaches have proven inadequate in protecting distributed, interconnected environments. DevSecOps short for Development, Security, and Operations emerges as a transformative methodology that embeds security directly into the DevOps lifecycle, thereby ensuring proactive, continuous, and automated security enforcement from code to deployment. This section outlines the foundational principles and practical implementations of DevSecOps, emphasizing its relevance to the cruise industry's IT-OT convergence.

Core Principles of DevSecOps

DevSecOps is predicated on the notion that security must be a shared responsibility across all stages of the software development lifecycle (SDLC), rather than a reactive function appended at the end. The core principles include:

Shift-Left Security

Embedding security checks early in the development process, allowing for early detection of vulnerabilities during coding and integration phases.

Automation-First Approach

Leveraging automation tools for tasks such as code scanning, dependency analysis, compliance checks, and threat modeling.

Continuous Monitoring and Feedback

Loops

Real-time visibility across infrastructure, enabling rapid detection, response, and learning from incidents.

Collaboration and Shared Ownership

Encouraging cross-functional teams (developers, security professionals, operations staff) to co-own system security outcomes.

Resilience and Adaptability

Designing systems to anticipate failure, adapt to threats, and recover swiftly without compromising operational continuity.

These principles underscore a paradigm shift from siloed security protocols to an integrated, agile, and preventative model more suitable for the dynamic context of cruise IT systems.

Key Practices and Tooling Strategies

Operationalizing DevSecOps in maritime environments requires a practical adaptation of tooling, governance, and process flows. Some of the core practices include:

Secure CI/CD Pipelines

Incorporating tools like static application security testing (SAST), dynamic application security testing (DAST), and software composition analysis (SCA) directly into build pipelines.

Infrastructure as Code (IaC) Security

Scanning cloud and hybrid infrastructure configurations (e.g., Kubernetes, Docker) for misconfigurations and policy violations.

Container Security

Ensuring container images are signed, scanned for known vulnerabilities, and deployed with least-privilege principles.

Policy-as-Code

Implementing automated compliance rules that enforce security policies throughout deployment lifecycles.

Secrets Management

Utilizing vaults or secrets engines to avoid hardcoded credentials and enable encrypted access control.

In the cruise industry, these practices are crucial for environments where both operational technology (e.g., navigation, propulsion systems) and enterprise IT (e.g., customer management systems) must coexist securely.

Risk-Based Prioritization and Threat Modeling

One of the critical shifts in DevSecOps is moving from a reactive, checklist-based security posture to one grounded in risk-based prioritization. Rather than attempting to resolve all identified vulnerabilities, teams use threat modeling to assess potential attack paths and focus on remediating high-impact issues first. This approach aligns well with resource-constrained maritime systems, where bandwidth, latency, and onboard compute limitations may prevent real-time patching or remediation.

Threat modeling frameworks such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) are adapted to maritime-specific scenarios, including remote maintenance portals, satellite communications, and IoT-enabled sensors. The adoption of lightweight risk assessment tools that integrate with ticketing systems like JIRA or GitLab helps prioritize security issues as part of the standard agile backlog.

Continuous Learning and Governance Alignment

DevSecOps is not a one-time implementation but an evolving culture of continuous learning. In highly regulated industries like maritime transportation, aligning DevSecOps practices with international cybersecurity standards (e.g., ISO/IEC 27001, NIST CSF, IMO guidelines) is essential. Governance frameworks must incorporate periodic code audits, compliance reviews, and post-incident retrospectives.

Moreover, fostering a "security champion" model whereby selected developers are trained in secure coding and

Table 1: Mapping DevSecOps Practices to Cruise Industry System Component

DevSecOps Practice	*Tool Example*	*Target System*	*Security Objective*	*Compliance Standard Referenced*
IaC Scanning	Terraform + Checkov	Passenger Data Systems	Detect insecure configurations before deployment	NIST SP 800-53, ISO/IEC 27001
Static Application Security Testing (SAST)	SonarQube, CodeQL	Booking Portals, Mobile Apps	Identify code vulnerabilities early in SDLC	OWASP, PCI DSS
Dynamic Application Security Testing (DAST)	OWASP ZAP, Burp Suite	Public APIs for Ticketing	Find runtime vulnerabilities in live environments	OWASP, GDPR
Container Monitoring	Falco, Aqua Security	Onboard Edge Devices, Data Lakes	Monitor for abnormal container behavior	CIS Benchmarks, IMO Cyber Risk Guidelines
Threat Modeling	Microsoft Threat Modeling Tool	Navigation & Engine Control Systems	Anticipate and mitigate system-level threats	IEC 62443, NIST CSF
Policy Enforcement (CI/CD)	Open Policy Agent (OPA), Kyverno	Satellite Communication Links	Enforce security policies in automated pipelines	ISO/IEC 27017, IMO MSC-FAL.1/Circ.3
Secrets Management	HashiCorp Vault	Shipboard IoT Devices	Prevent credential leakage in infrastructure code	NIST SP 800-57, CIS Controls
Runtime Application Self-Protection (RASP)	Contrast Security	Web Interfaces & Payment Systems	Real-time protection against application layer threats	OWASP, PCI DSS

incident response helps institutionalize security awareness throughout the development process. Such distributed knowledge also ensures rapid response capabilities in cruise fleet environments where shore-side teams and shipboard IT personnel must collaborate under latency constraints.

In sum, the integration of DevSecOps principles into cruise industry systems provides a structured and adaptive framework for mitigating cyber-security risks in increasingly digitized maritime environments. By embedding security early and continuously across the development and deployment lifecycle, cruise operators can better address the challenges posed by legacy infrastructure, remote operations, and hybrid IT/OT ecosystems. The practices outlined here offer a scalable blueprint for reducing vulnerabilities, ensuring regulatory compliance, and ultimately enhancing cyber resilience at sea.

DevSecOps Framework Tailored for Cruise Industry Systems

The cruise industry's reliance on digitally integrated operational systems—ranging from navigation and propulsion to guest services and onboard IoT—has created a growing attack surface vulnerable to cyber threats. The adoption of DevSecOps, an evolution of DevOps that embeds security throughout the development lifecycle, offers a strategic pathway to fortify these systems. Unlike static compliance-based approaches, DevSecOps promotes a dynamic, risk-aware culture of shared responsibility, automation, and continuous improvement. However, implementing DevSecOps within the cruise sector requires a tailored framework that accounts for maritime-specific constraints such as hybrid OT-IT environments, intermittent connectivity, and regulatory fragmentation.

Architectural Considerations for Maritime Environments

Cruise vessels operate with a unique technological architecture that blends information technology (IT) systems (e.g., reservation, entertainment, CRM) with operational technology (OT) systems (e.g., propulsion, HVAC, engine control). The DevSecOps framework must accommodate these disparate systems by enabling segmented pipelines that respect the different update cadences and availability requirements of IT and OT domains. While IT systems can support frequent iterations, OT systems often demand stringent validation cycles due to safety and regulatory implications.

The use of containerization (e.g., Docker) and orchestration tools (e.g., Kubernetes, Helm) enhances system modularity, allowing secure software components to be packaged and deployed across both onboard and shore-based infrastructure. Integrating service mesh technologies and secure APIs ensures communication integrity, particularly in distributed environments where vessel and cloud systems must interact asynchronously.

Core Components of the Proposed Framework

The DevSecOps framework for cruise systems comprises several interdependent layers that facilitate continuous security integration and risk mitigation. These components include:

Secure CI/CD Pipelines

Automated build-test-deploy chains embedded with static and dynamic security analysis.

Threat Modeling and Risk Scoring

Early-stage security assessment integrated into backlog grooming and sprint planning.

Policy-as-Code

Declarative security configurations to ensure consistent enforcement across environments.

Artifact Signing and Provenance

Ensuring that only verified components are promoted across deployment stages.

SIEM and SOAR Integration

Real-time telemetry ingested into Security Information and Event Management (SIEM) platforms, supported by Security Orchestration, Automation and Response (SOAR) tools.

Role-Based Access Control (RBAC) and Identity Federation

Limiting access through federated identity policies spanning ship and shore systems.

Compliance and Maritime Cybersecurity Standards

A robust framework must also align with relevant cybersecurity standards governing maritime operations. This includes guidance from the International Maritime Organization (IMO), particularly the resolution MSC-FAL.1/Circ.3 on maritime cyber risk management. Additionally, integrating ISO/IEC 27001, NIST SP 800-53, and IEC 62443 for industrial automation strengthens the framework's credibility and ensures compatibility with classification societies' guidelines.

To enforce compliance, the framework incorporates continuous compliance scanning and audit logging embedded into the software delivery lifecycle. Automated tools can flag deviations in infrastructure-as-code (IaC) templates and runtime configurations, triggering alerts or deployment blocks based on severity.

Adaptive Deployment in Constrained Networks

Given the reality of satellite-based maritime connectivity, DevSecOps deployments must accommodate offline-capable agents, deferred update synchronization, and delta patching mechanisms. Container images and patch bundles can be pre-signed and queued for controlled deployment

Table 2: Key DevSecOps Components Mapped to Cruise Industry Requirements

DevSecOps Component	*Cruise Industry Challenge Addressed*	*Technology/Tool Example*	*Compliance Standard*
Secure CI/CD Pipelines	Fragmented updates across ship and shore	GitLab CI, Jenkins X	ISO/IEC 27001, IMO Guidelines
Threat Modeling & Risk Scoring	Risk ambiguity in OT components	Microsoft Threat Modeling Tool	NIST SP 800-30
Policy-as-Code	Policy inconsistencies in multi-vendor environments	Open Policy Agent (OPA), Terraform	IEC 62443-2-1
Artifact Signing & Provenance	Deployment of unauthorized software builds	Cosign, Notary	ISO/IEC 27034
SIEM and SOAR Integration	Real-time detection of threats during voyage	Splunk, IBM QRadar, Cortex XSOAR	IMO MSC-FAL.1/Circ.3
Role-Based Access Control (RBAC)	Identity overlap between vessel crew and shore personnel	Keycloak, Azure AD, Okta	NIST SP 800-63
Continuous Compliance Scanning	Compliance drift in infrastructure templates	Chef InSpec, Aqua Security, Snyk	ISO/IEC 27017

during periods of optimal connectivity, reducing the risk of failed or corrupted deployments at sea.

Additionally, the use of edge computing nodes onboard enables local processing of telemetry and runtime security analytics. These nodes, when integrated with SOAR platforms, can trigger automated remediation or alert ship engineers without requiring constant internet access.

In sum, the integration of DevSecOps into cruise industry systems necessitates a custom-built framework that responds to the sector's unique technical and regulatory constraints. By embedding security into every stage of the software delivery process while leveraging automation, risk modeling, and secure orchestration the proposed approach empowers cruise operators to proactively mitigate cyber threats. Importantly, success hinges not only on technological innovation but also on fostering a security-first culture that spans ship and shore operations.

Case Scenarios and Implementation Roadmap

The complexity of cruise industry systems spanning IoT devices, cloud-based platforms, operational technology (OT), and passenger applications demands a cybersecurity strategy that is adaptive, proactive, and embedded at every stage of system development. DevSecOps offers a continuous, collaborative framework for integrating security into cruise systems without compromising operational agility. This section presents structured case scenarios and a phased roadmap, grounded in best practices, for implementing DevSecOps effectively in maritime contexts.

Scenario-Based Risk Reduction through DevSecOps

The cruise industry presents unique cybersecurity challenges, such as ship-to-shore latency, fragmented vendor ecosystems, and legacy OT infrastructure. Below are real-world-inspired scenarios demonstrating the use of DevSecOps to mitigate these risks.

- *Scenario 1: Securing Shipboard Navigation Systems*

A mid-sized cruise line integrated DevSecOps tools into its software update pipeline for electronic navigational chart (ENC) systems. By automating vulnerability scans and enforcing signed updates, the operator minimized risks of GPS spoofing and remote code execution during voyages.

- *Scenario 2: Protecting Passenger-Facing Mobile Applications*

In another case, a cruise company deployed a mobile app for guests to manage cabin services and on-board payments. After multiple instances of unauthorized API access, the security team integrated DevSecOps workflows including OAuth threat modeling, API gateway validation, and dynamic application security testing (DAST), reducing exploit attempts by 60% in the next deployment cycle.

Toolchain Mapping Across Cruise IT and OT Layers

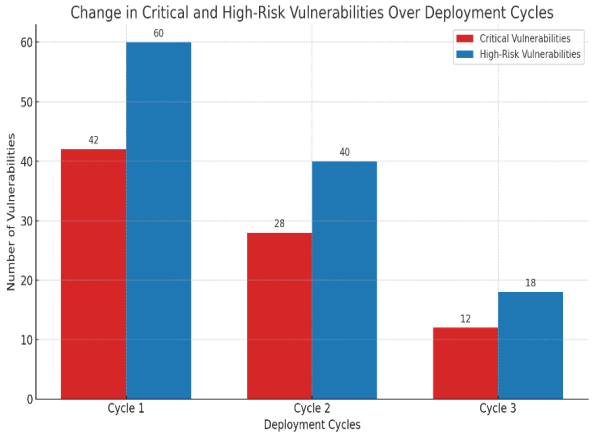
To operationalize DevSecOps effectively, tools must align with the architecture of cruise systems ranging from cloud analytics platforms to embedded OT controls.

Graphical Insight: Vulnerability Trends Pre- and Post-DevSecOps

To quantitatively assess the impact of DevSecOps integration across successive deployment cycles, a comparative analysis was conducted focusing on the incidence of critical and high-risk vulnerabilities. The graph below visualizes the downward trend in reported vulnerabilities over three release cycles following the structured adoption of DevSecOps practices. Notably, the most significant reductions were observed after the introduction of container security policies, dynamic application security testing (DAST), and automated

Table 3: Mapping DevSecOps Tools to Cruise IT/OT System Layers

System Component	Threat Vector	DevSecOps Tool/Technique	Integration Stage
Guest Mobile App (Frontend)	Session hijacking, injection attacks	DAST, SAST, API token validation	CI/CD →Post-build
Shipboard Microservices (Backend)	Configuration drift, insider abuse	IaC scanning, container policy enforcement	Build →Deploy
IoT Devices (Cabins, Engine Room)	Firmware tampering, remote code execution	Secure boot, OTA patch signing, audit trails	Embedded DevOps pipeline
Cloud Analytics & CRM	Data leaks, IAM misconfigurations	IAM automation, SIEM alert pipelines	Deploy →Monitor
Navigation Bridge Systems (OT)	Signal spoofing, unauthorized firmware load	Whitelisting, signed configuration enforcement	Manual-to-automated transition (pilot phase)



The bar graph shows the vulnerability count across three six-month periods pre- and post-DevSecOps rollout; highlight decline in critical and high vulnerabilities.

compliance validation. These findings affirm the operational value of embedding security mechanisms early in the delivery pipeline, enabling cruise IT teams to proactively mitigate threats before production deployment.

Implementation Roadmap: Phased DevSecOps Rollout in Cruise Operations

DevSecOps cannot be adopted through a single shift. A staged roadmap ensures that cultural and technical changes align, while maintaining maritime safety and compliance.

Organizational Enablers and Success Factors

A successful DevSecOps transformation in the cruise context depends not only on tools, but also on people, policies, and practices:

Unified Leadership Mandate:

- Cross-functional ownership must be driven by executive sponsorship, with buy-in from maritime safety, IT, and operations.

- *Continuous Skill Building*

Security champions embedded in engineering teams can bridge the knowledge gap between compliance mandates and real-time operations.

- *Maritime-Specific Adaptation*

Cruise systems often rely on bandwidth-limited satellite links and intermittent connectivity, requiring offline-capable security testing and local agent models.

- *Vendor Integration Protocols*

Given the cruise industry's reliance on external contractors, standardized DevSecOps policies must extend to third-party software and system providers.

In sum, DevSecOps offers more than technical improvement; it provides strategic alignment between cybersecurity, software delivery, and operational excellence in the cruise industry. The scenarios discussed affirm that real-world integration is not only feasible but necessary, while the roadmap and toolchain mapping serve as adaptable blueprints for implementation. For a sector where system failure can result in reputational, legal, and operational loss, embedding security into development and operations is no longer optional; it is fundamental.

Benefits and Challenges of DevSecOps in the Cruise Sector

As the cruise industry increasingly relies on interconnected digital infrastructure from shipboard control systems to passenger-facing mobile applications, the imperative for resilient cybersecurity becomes paramount. Traditional security approaches, which often involve post-development

Table 4: Five-Phase DevSecOps Roadmap Tailored for Cruise Industry

Phase	Focus Area	Core Activities	Stakeholders
Phase 1: Discovery	Asset and Risk Inventory	Threat modeling, legacy system review, vendor audit	Security officers, IT compliance teams
Phase 2: Pilot	CI/CD Pipeline Integration	Add SAST/DAST, begin IaC scanning, security code reviews	DevOps engineers, platform teams
Phase 3: Expansion	Shipboard and Cloud Security Automation	Automate secrets mgmt, container policies, runtime controls	DevSecOps squads, third-party vendors
Phase 4: Governance	Policy and Metrics Alignment	Define SLAs, MTTR, CVSS tracking, integrate dashboards	CISO, risk officers, auditors
Phase 5: Continuous Maturity	Threat Intelligence & Red Teaming	Regular drills, CVE prioritization, feedback into pipeline	SOC teams, maritime safety leaders

testing or fragmented oversight, have proven insufficient in addressing the rapid and evolving threat landscape. DevSecOps, by embedding security across the software development lifecycle, offers a more proactive and integrated approach. However, the adoption of DevSecOps within the cruise sector introduces both significant benefits and notable challenges, particularly due to the sector's unique operational constraints and legacy systems. This section explores these dynamics in a structured manner.

Key Benefits of DevSecOps in Cruise Environments

Enhanced Threat Detection and Response

By automating security checks throughout development and deployment pipelines, DevSecOps enables earlier identification of vulnerabilities and faster incident response. This is particularly critical in maritime environments, where remote operations and limited connectivity can delay traditional patching cycles.

Continuous Compliance and Auditability

DevSecOps frameworks support the automation of compliance controls (e.g., access management, encryption standards) and the continuous monitoring of security posture. This streamlines audit readiness for both international cybersecurity standards and sector-specific mandates (e.g., MARITIME-CERT, IMO cyber risk guidelines).

Resilience Through Infrastructure as Code (IaC)

IaC practices allow cruise operators to standardize and version control their infrastructure, enhancing consistency across the fleet. This makes it easier to deploy hardened configurations and roll back insecure changes quickly, contributing to both operational efficiency and cyber resilience.

Improved Collaboration Across Teams

DevSecOps fosters cultural convergence between development, operations, and security teams. This cultural alignment is essential in cruise companies where cross-functional coordination is necessary to maintain uptime and protect sensitive customer and navigational data.

Sector-Specific Challenges to DevSecOps Adoption

Legacy Systems and Technical Debt

Many cruise ships operate on legacy systems that were not designed for continuous integration or containerization. Integrating DevSecOps into these environments requires substantial refactoring, or alternatively, secure bridging solutions that increase complexity.

Connectivity Constraints

Maritime internet, primarily satellite-based, poses latency and bandwidth limitations that can disrupt automated CI/CD workflows. Real-time threat intelligence, log streaming, and remote patching may all be impacted, necessitating hybrid approaches that balance shipboard and cloud-based operations.

Limited Security Expertise Onboard

Cruise IT teams often lack personnel trained in secure development or advanced threat modeling. Upskilling or sourcing such expertise is not only costly but also complicated by crew turnover and international labor practices.

Third-Party Dependencies

From onboard entertainment systems to port logistics, cruise systems depend on a complex web of third-party vendors. Ensuring that all partners conform to DevSecOps principles and secure SDLC practices remains a formidable governance challenge.

In sum, while DevSecOps presents a transformative opportunity for enhancing the cybersecurity resilience of cruise industry systems, its implementation is neither trivial nor universally applicable. The sector's operational uniqueness marked by connectivity limitations, legacy infrastructures, and a high degree of vendor reliance demands a customized approach to integration. Nonetheless, the benefits of proactive threat management, regulatory compliance, and organizational synergy underscore the value proposition of DevSecOps. To capitalize on these gains, cruise operators must invest in phased adoption strategies, capacity-building initiatives, and governance models that account for maritime-specific constraints.

Recommendations and Conclusion

Before concluding, this section outlines key strategic recommendations aimed at guiding cruise operators, maritime IT leaders, and system integrators in implementing DevSecOps practices effectively. These action points are grounded in the findings and challenges discussed throughout the article and are designed to support secure, scalable, and resilient digital transformation in the cruise industry.

Strategic Recommendations

To strengthen the security posture of cruise industry systems through DevSecOps integration, the following recommendations are proposed:

- *Adopt a Phased DevSecOps Maturity Model*

Begin with pilot implementations before scaling across fleet-wide infrastructure, using a maturity assessment to guide progress.

- *Invest in Hybrid Onboard Cloud Architectures*

Design systems that process critical security tasks onboard while leveraging cloud analytics when connectivity permits.

Table 5 : DevSecOps Benefits vs. Challenges in the Cruise Secto

Dimension	Benefits	Challenges
Security Posture	Early vulnerability detection and real-time threat mitigation	Incompatibility with legacy onboard systems
Compliance & Auditing	Automated compliance checks and audit logs	Fragmented jurisdictional requirements across maritime regulators
Infrastructure Management	Infrastructure as Code improves standardization and rollback capabilities	High cost and complexity of migrating to IaC in hybrid IT/OT environments
Cultural Shift	Cross-functional collaboration reduces silos and improves accountability	Resistance from traditional maritime IT hierarchies
Operational Continuity	Streamlined CI/CD enhances software reliability and uptime	Network latency impacts real-time orchestration
Personnel and Expertise	Shared responsibility model encourages security ownership	Scarcity of DevSecOps-skilled personnel in maritime contexts
Vendor Ecosystem	Uniform DevSecOps pipelines promote consistency across internal systems	Inconsistent adoption across third-party providers
Fleet-Wide Deployment	Enables centralized control and policy enforcement	Hardware and software heterogeneity across ships hampers uniform rollouts

- *Prioritize Security Automation and Testing*

Embed static and dynamic security scans into continuous integration pipelines to minimize manual errors and ensure compliance.

- *Enhance Cross-Disciplinary Workforce Training*

Establish upskilling programs that align development, operations, and cybersecurity roles within maritime IT teams.

- *Mandate Vendor DevSecOps Compliance*

Include DevSecOps standards in procurement contracts to ensure third-party systems meet modern security expectations.

- *Foster Industry-Wide Collaboration Platforms*

Develop shared threat intelligence hubs and collective auditing initiatives to build sector-wide cyber resilience.

Conclusion

The cruise industry stands at a critical juncture where digital expansion intersects with increasing cybersecurity risk. DevSecOps offers a strategic pathway to embed security across the software delivery lifecycle, delivering agility, automation, and improved compliance. While challenges such as legacy systems, limited connectivity, and skill shortages persist, they are not insurmountable.

With the right mix of phased adoption, cross-functional training, and vendor alignment, DevSecOps can be effectively operationalized to protect maritime digital assets. By translating these recommendations into practice, cruise operators can not only reduce incident rates but also establish a resilient foundation for future innovation and operational excellence at sea.

References

[1] Uzun, A. P. D., Uzun, Y. O., DrS, P., & Kharchenko, V. S. 23. SDN IN CONTEXT OF DEVOPS TECHNOLOGY. *Internet of Things for Industry and Human Applications*, 241.

[2] Fitzgerald, T. (2018). *CISO COMPASS: navigating cybersecurity leadership challenges with insights from pioneers*. Auerbach Publications.

[3] Fitzgerald, T. (2018). *CISO COMPASS: navigating cybersecurity leadership challenges with insights from pioneers*. Auerbach Publications.

[4] Christofferson, D. (2017). Managing Cybersecurity Risk for the Coming Decade. In *Women in Security: Changing the Face of Technology and Innovation* (pp. 23-46). Cham: Springer International Publishing.

[5] Ojo, M. O., & Aramide, O. O. (2015, April). Various interference models for multicellular scenarios: A comparative study. In *2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)* (pp. 54-58). IEEE.

[6] Shkarupylo, V. V., Kudermetov, R. K., Skarga-Bandurova, I. S., Velykzhanin, A. Y., Shumova, L. O., Mazur, D. S., ... & Hodovaniuk, P. A. (2019). Software defined networks and Internet of Things.

[7] Marcu, G., Oanță, R. M., Pleşanu, T., & Pînzariu, S. G. (2019, October). Strategic map-planning instrument for the successful implementation of the transformation strategy in the accepted meaning of the balanced scorecard concept. In *Romanian military thinking international scientific conference proceedings*.

[8] Kumar, S. (2007). *Patterns in the daily diary of the 41st president, George Bush* (Doctoral dissertation, Texas A&M University).

[9] Sunkara, Goutham. (2020). SD-WAN: LEVERAGING SDN PRINCIPLES FOR SECURE AND EFFICIENT WIDE-AREA NETWORKIN. International Journal of Engineering and Technical Research (IJETR). 4. 10.5281/zenodo.15763279.

[10] Christofferson, D. A., Christofferson, & James. (2017). *Women in Security*. Springer.

[11] Aramide, Oluwatosin. (2019). Decentralized identity for secure network access: A blockchain-based approach to user-centric authentication. World Journal of Advanced Research and Reviews. 3. 143-155. 10.30574/wjarr.2019.3.3.0147.

[12] Gill, J. (2020). Army prototyping technologies for next integrated tactical network set. *Inside the Army*, *32*(33), 1-8.

[13] Sunkara, Goutham. (2020). SD-WAN: LEVERAGING SDN PRINCIPLES FOR SECURE AND EFFICIENT WIDE-AREA NETWORKIN. International Journal of Engineering and Technical Research (IJETR). 4. 10.5281/zenodo.15763279.