CASE STUDY

cybercrucible

PROTECTING the Seas

A Real-World Case of Cyber Resilience

When a well-known global cruise and sightseeing company expanded operations through acquisition, it inherited more than just vessels—it inherited a silent, persistent cyber breach. **That's when Cyber Crucible stepped in.**

From sleek local sightseeing ships to cruise liners sailing beyond the horizon, this fleet operated in some of the most connectivity-challenged environments on Earth. Ships in port communicated over traditional networks, while those at sea relied on finicky satellite and radio modems—bursting data when signals allowed. It was a perfect storm of complexity, remoteness, and vulnerability.

Enter Cyber Crucible...

Brought in after an undisclosed breach came to light post-acquisition, Cyber Crucible was deployed across vessels with zero room for error. Within hours, it was actively detecting and deflecting threats—without the need for onboard IT staff.

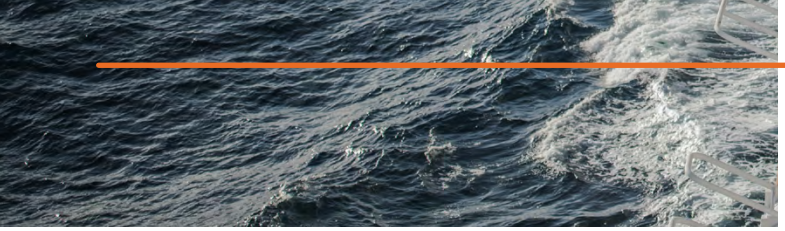
How Cyber Crucible saved this client time, money, and reputation:

- **Avoided costly incident response delays** by acting immediately, autonomously.
- **Prevented further spread of the breach**, protecting customer and operational data.
- **Preserved critical forensic logs**, enabling cost-effective post-incident analysis.
- **Mitigated reputational damage** by swiftly halting attacker access before wider exposure.

Within hours, Cyber Crucible was actively detecting and deflecting threats.

CONTACT

+1 (412) 775.2158 info@cybercrucible.com www.cybercrucible.com



WHY CYBER CRUCIBLE Worked at Sea

- **Autonomous Response:** Operated independently, even during multi-day voyages without IT teams.
- **Forensic Data Retention:** Preserved rich forensic logs for post-voyage analysis, even when disconnected for long stretches.
- **Edge-First Security:** Delivered full-spectrum protection without needing constant connectivity.
- **Satellite Smart:** Adapted to low-bandwidth, bursty satellite transmissions and weather-related interruptions.
- **Built to Endure:** Stayed resilient—even when attackers tried to shut it down or degrade its performance.
- **The Bigger Picture:** The compromised systems ranged from passenger-facing recreational terminals to mission-critical maritime controls. Cyber Crucible quickly became the silent guardian, quietly holding the line where traditional cybersecurity stacks had failed.

Then Came a Twist...

Cyber Crucible's logs revealed something unusual: presence and activity from U.S. military and federal law enforcement personnel—undisclosed, yet unmistakable. It became clear this was no ordinary breach. Nation-state attackers were likely involved, focusing only on ships operating in international waters. Domestic sightseeing vessels were completely untouched.

The Final Escalation

Cyber Crucible fended off attacker attempts to infiltrate and sabotage. When traditional intrusion tactics failed, the adversaries escalated:

1. After previous attempts to bypass Cyber Crucible, they hijacked Windows login credentials.
2. Then, they accessed BIOS-level settings, remotely locking systems before boot-up.
3. With systems halted before the OS could load, Cyber Crucible's defense was effectively caged.

Despite this, the solution never stopped protecting until the very last breath of system access. Ultimately, the affected machines had to be physically decommissioned. But not before Cyber Crucible proved its worth.

Solution Outcomes

Blocked advanced attacks for over a month—autonomously.	**Forced attackers to target firmware—proof of strength.**
Edge-first design proven ideal for maritime use.	**Saved time and money through early, ongoing protection.**

The Conclusion

In a world where oceans can hide adversaries and distance can delay response, Cyber Crucible delivered fast, reliable, and resilient protection when it mattered most. For the maritime industry—and any edge-first environment—it's more than security. It's an investment in uptime, safety, and cost-savings—even off the grid.