



The sales team at Rapid7 showed us what InsightConnect could do, above and beyond its built-in workflows”

Xerxes Kiok Kan, Head of Information Security (CISO), Anglo-Eastern

Industry

Services

Region

APAC

Products

InsightIDR,
InsightVM,
InsightConnect

Securing the Digital Open Waters of Maritime Shipping



Overview

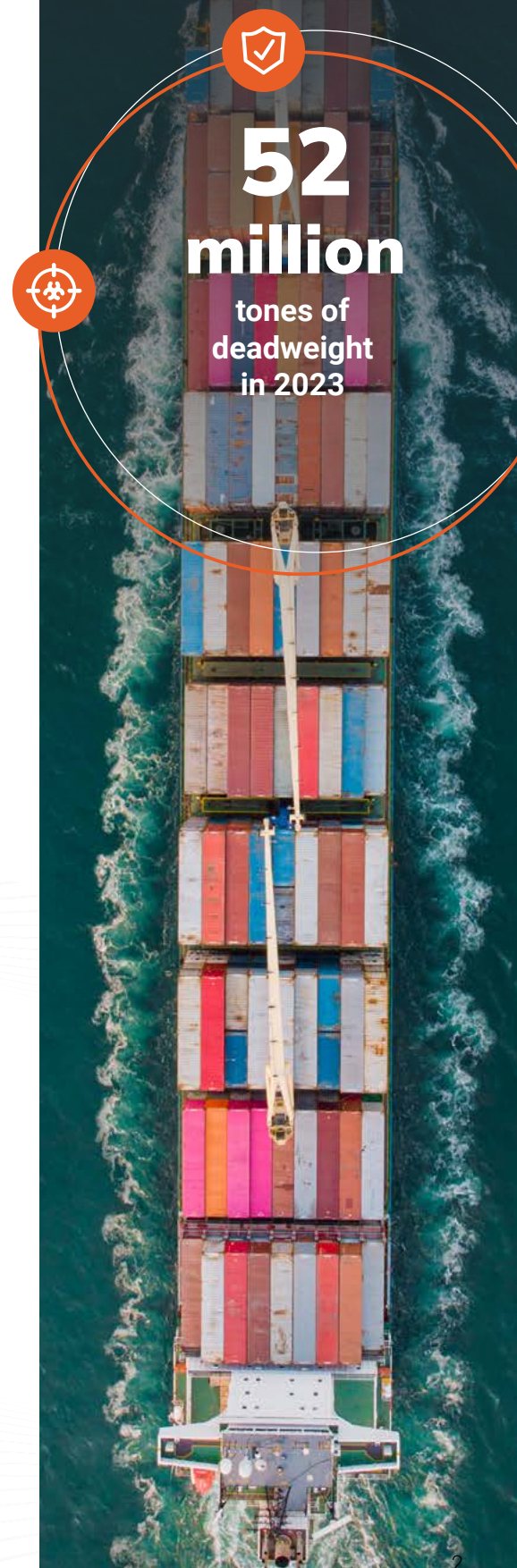
Company

Anglo-Eastern has a unique challenge in today's landscape: Keep one foot in the old world of heavy-goods shipping and plant the other foot firmly in the new world of securing the modern networking infrastructure transforming its industry.

One of the world's leading suppliers of independent ship-management, Anglo-Eastern, services close to 650 sea-faring vessels worldwide, from oil tankers to passenger cruise ships. The company is committed to shaping a better maritime future by nurturing the global network of communities in which they operate.

Challenge

This commitment to the physical places is part of their digital challenge. If cyber operations can't be secured, there certainly won't be a subsequent positive impact on their frequented local communities. So, just how big of a physical presence does Anglo-Eastern manage? "Deadweight tonnage" is the amount of weight a cargo ship can carry, and the ships under the company's management carried 52 million tons of deadweight in 2023. That's a "ton" of impact and influence all over the world, which means a huge cyber presence to secure.



Solution

Setting the sea(ne)

Anglo-Eastern's managed ships are constantly moving, which makes a coordinated cybersecurity effort a real challenge as they navigate in and out of various jurisdictions and international territories.

For the company, this resulted in a patchwork of cybersecurity policies and practices – and an IT team overwhelmed by manual, time-intensive processes.



We spent a lot of time undertaking administrative tasks.”

Xerxes Kiok Kan, Head of Information Security (CISO), Anglo-Eastern

“For example, our engineers had to constantly look at the console, see if there is a new device and assign that device to the right group. In some cases, they were staying up until three or four in the morning handling these tasks,” Xerxes continued. This, in turn, increased the risk of human error, necessitating a change in approach.

What's a CISO to do?

Let's reiterate the enormity of the challenge facing Anglo-Eastern's IT and network security teams: The company's ships are reaching an average of 60 ports-of-call every 24 hours. With his team of humans maxing out on exhaustion, Xerxes knew automation was the way forward. Turning to Rapid7's InsightConnect solution, the security team at Anglo-Eastern was able to implement workflows that helped streamline repetitive and time-consuming tasks. This freed the team up to take on higher-value, more strategic work that could really start to propel efficiencies – and ships.



The sales team at Rapid7 showed us what InsightConnect could do, above and beyond its built-in workflows”, says Xerxes. “It became clear that with APIs and some Python developer skills, so much was possible.”



Our engineers had to constantly look at the console, see if there is a new device and assign that device to the right group. In some cases, they were staying up until three or four in the morning.”

Xerxes Kiok Kan,
Head of Information Security (CISO), Anglo-Eastern

Anglo-Eastern's IT teammates are now freed up from the demands of monitoring and managing the minutiae of their cybersecurity systems. Their efforts are aided by the accurate, company-wide data generated by InsightConnect. This enables Xerxes and the cybersecurity team to uncover insights and prioritize response strategies in a time-efficient manner.

This data can also help to quickly address customer or regulator audits – an increasingly frequent occurrence in the maritime industry. This helps to create efficiencies with technical and operations teams who are able to optimize machinery and voyages while ensuring compliance with industry regulations.

With improvements to the company's overall threat protection stance now going full steam, Anglo-Eastern is primed and ready to respond to the increasing spectre of attackers who aren't demanding to board their ship in the physical sense.

Anglo-Eastern sets sail with Threat Complete

A great challenge still facing Anglo-Eastern is that of managing various kinds of workstations and servers across 650 different types of vessels, many of which are simultaneously out on the open sea. Therefore, it makes perfect sense that next up for the company's IT and cybersecurity teams is breaking down the silos created by one-off solutions designed to address individual functions.

They are looking to Rapid7's Threat Complete offering – which includes InsightIDR, InsightVM, and InsightConnect – to help automate cybersecurity on seaborne vessels. This single-subscription offers a clear view into the kill chain as well as a number of challenges facing modern SOCs:

- Tool sprawl
- Budget pressures
- Little time for proactive security measures



**Think of it this way:
One ship is equivalent
to one office”**



Xerxes continues: “The problem is that we don’t have an IT department on each ship, nor an on-site SOC, yet incidents can happen at any time”. Threat Complete solutions – including [InsightIDR](#) and [InsightVM](#) – will have an important role to play in driving transformation on this issue, as Xerxes recognizes these systems are only as capable as the staff operating them on the high seas.

“A company whose ships are in constant motion, sailing all over the world, needs cybersecurity solutions that are also in constant motion.



Whether it’s continuous assessment of a dynamic attack surface for vulnerabilities with InsightVM or strengthening security postures with InsightIDR and InsightConnect to fend off threats before they can gain a foothold, Threat Complete helps steady Anglo-Eastern’s digital operations before the waters can get too rough. Rapid7 is here for that.”

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research—using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what’s next.



View all of our customer success stories.

CUSTOMERS STORIES

RAPID7

PRODUCTS

- Cloud Security
- XDR & SIEM
- Threat Intelligence
- Vulnerability Risk Management

- Application Security
- Orchestration & Automation
- Managed Services

CONTACT US

[rapid7.com/contact](https://www.rapid7.com/contact)

To learn more or start a free trial, visit: <https://www.rapid7.com/try/insight/>