CUSTOMER CASE STUDY

How Zakher Marine International benefits from security expertise and an open approach

ZMi | HOLDINGS

Industry
Maritime Offshore

Sophos Solutions
Sophos Managed Detection and Response (MDR)

SOPHOS

About Zakher Marine International

Zakher Maritime International (ZMI Holdings) is a global maritime organization that provides services to the marine and offshore oil and gas industries. This includes vessel chartering and management, supported by a fleet of barges and offshore support vessels.

The challenges

- Seeking comprehensive security solutions to assess global risk.
- Enabling strong incident response capabilities.
- Meeting various regional compliance regulations.

Aditya Kaushik joined ZMI as ICT Director in June 2022 and began evaluating the company's current technology systems, looking at their ability to detect and respond to potential cyber threats.

Strengthening the organization's security posture is critical, as is improving their overall compliance framework.

"As a maritime organization, we have a significant need for compliance with maritime frameworks," Kaushik said. "Since our vessels operate in international waters, we must adhere to numerous regulations set by maritime authorities, which adds substantial complexity to our cybersecurity framework."

This served as a starting point to evolve the organization's security strategy and determine a path forward.

"We wanted to understand the overall landscape of our organization," Kaushik said. "Where we operate, where the risks originate from, whether they are onshore or offshore — and specifically, how we implement solutions that would align not only with industry standards, but also with the specific maritime controls that we have to comply with."

The solution

- Provide a global view of threats.
- Fill in-house cybersecurity talent gaps.
- Deliver a holistic MDR solution with proactive threat hunting, log storage, and full-service incident response.

"As a maritime organization, we have a significant need for compliance with maritime frameworks. Since our vessels operate in international waters, we must adhere to numerous regulations set by maritime authorities, which adds substantial complexity to our cybersecurity framework."

Aditya Kaushik
ICT Director, ZMI Holdings

SOPHOS

Sophos Managed Detection and Response (MDR) provides ZMI with a fully managed solution that combines extensive security expertise with an open, powerful system for 24/7 threat monitoring, detection, investigation, and response — all fuelled by advanced analytics. ZMI's security team can engage Sophos security analysts within 90 seconds via live chat.

"Sophos serves as our security operations center," Kaushik said. "It augments the gap in skill sets or resources that we have in house."

This direct around-the-clock access to security expertise results in rapid response to any threat detected. Investigations are infused with powerful proprietary threat intelligence from Sophos X-Ops Counter Threat Unit (CTU) research team, along with findings from a variety of expert Sophos teams that perform threat hunting, incident response, and security testing engagements. Sophos seamlessly integrates with hundreds of leading security technology sources across endpoint, network, cloud, identity, OT, email, and business applications.

"Sophos has a very inclusive open platform approach which allows us to integrate all our other security solutions, so we are able to measure risk and threats that are coming from different applications within our environment," Kaushik said.

To help ZMI with compliance, Sophos MDR includes one year of raw telemetry storage by default, making logs easily accessible as needed. The solution also includes monthly threat hunts across ZMI's environment to increase vigilance against stealthy threats. Sophos features a fully transparent user interface, making collaboration between the ZMI team and Sophos resources seamless and helping to accelerate learning and knowledge transfer.

"Their response time is brilliant. We get quite a lot of engagement with various teams within Sophos, which helps us to have that assurance that they are continuously monitoring what's happening within our environment."

Aditya Kaushik
ICT Director, ZMI Holdings

Results and impact

- Integration of other solutions and technology via an open, transparent system.
- Rapid response to threats and proactive engagement with Sophos resources.
- Global perspective on the threat landscape.

Working with Sophos since the start of 2023, ZMI has gained a view of the global threat landscape that would have been difficult to achieve alone. Kaushik stresses how critical this is in assessing how external threats impact companies like ZMI with operations around the world.

"Sophos understands the challenges at the global level," Kaushik explained. "Generally, an in-house team tends to focus more on the threats that are within your perimeter and the environment they operate in. But when you work with a global partner, it tends to give you that wider understanding of what the threats could be and how to proactively address areas of risk and vulnerability."

Looking ahead

Kaushik cited a strong Sophos in-region presence and responsiveness to threats as reasons for choosing Sophos MDR.

"Their response time is brilliant," Kaushik said. "We get quite a lot of engagement with various teams within Sophos, which helps us to have that assurance that they are continuously monitoring what's happening within our environment. Their incident response discipline is critical. Knowing what the SOC team can do in the event of a threat or an incident provides reassurance."

Selecting Sophos MDR has enabled ZMI to reduce their risk, strengthen their team's capabilities, and better meet the organization's compliance requirements.

"Sophos serves as our security operations center. It augments the gap in skill sets or resources that we have in house."

Aditya Kaushik
ICT Director, ZMI Holdings

To learn more visit Sophos.com

SOPHOS