

Protecting the Maritime Domain

In alliance with our members and their mission to patrol, protect and preserve the Nation's maritime domain, its infrastructure and its economic heartbeat vital to the United States, the NMLEA has identified RiskSense as a STAR Product.

With a unique background and capabilities developed through U.S. Department of Defense and National Security Agency funding, RiskSense has pioneered a higher-level capability called **cyber risk management**.



The RiskSense platform does not replace the cyber security tools and processes being used currently in an organization. Rather, the platform **augments and extends cyber security capabilities by prioritizing risk, applying unique threat intelligence, and accelerating the remediation process**; a real plus for small IT teams trying to deal with a growing attack surface. Especially in the maritime industry.

As recent alerts from the U.S. Coast Guard indicate, the maritime industry is an attack surface that keeps growing daily through cruise ship passenger experiences, speed of shipping services, digital navigational connectivity, and electronic billing procedures to name but a few. All this and the Internet of Things has created a multitude of vulnerabilities, increasing access points and plentiful targets throughout our maritime world. All of which presents an appealing opportunity to our adversaries with great potential reward and critical impact on our port driven organizations individually, and our economy as a whole.

Now, through the RiskSense platform, maritime organizations from port authorities to shipping companies to cruise lines, can all become **proactive, versus reactive**. As IT personnel continue to get overwhelmed by the information flow, RiskSense can provide its leaders, supervisors and managers with a "single pane" view of their environment, and visually cue their organization's "RiskScore," having a better handle on what are priorities and criticalities. All without increasing their staff costs, but rather, saving costs.

To learn more about how the RiskSense Platform can impact your organization and its Cyber Risk Management capabilities, or to arrange a free test of the platform in your environment (so you can see what it sees), contact the Academy staff at cyber@nmlea.org.



An NMLEA STAR Product

Who is RiskSense?

RiskSense is not in cyber security, but rather cyber risk management. With its DNA coming out of work with DoD and NSA, RiskSense works with Federal, State and corporate entities to rapidly improve and then sustain a higher cyber security posture.

- *RiskSense founder was part of a think tank that collaborated with the U.S. Department of Defense and U.S. Intelligence Community on applying some of the first AI concepts to cybersecurity problems (e.g. as part of the CACTUS Program - Computational Analysis of Cyber Terrorism against the U.S.).*
- *RiskSense is rapidly building a client footprint across major industry sectors including Worldpay (credit card processor), Crane Merchandising Systems (smart vending provider, e.g. Coke & Pepsi), Assa Abloy (world's largest lock manufacturer), Equifax (data analytics and technology company – after the breach), State of Arizona (Governor Ducey uses it across all his agencies) and may others.*
- *Our nationally recognized cyber threat intelligence was highlighted last year when RiskSense provided the first national warning about the WannaCry attack (RiskSense clients had early warning). See DOJ Indictment, page 106 <https://www.justice.gov/opa/press-release/file/1092091/download>*

Pioneered Cyber Risk Management

Company	<ul style="list-style-type: none">• Founded in 2015, Sunnyvale, CA and Albuquerque, NM• CACTUS (US Congress): Computational Analysis of Cyber Terrorism against the US• NSA/DHS National Academic Centers of Excellence• Early Warning of WannaCry and Developed First RFID Fragmented Malware
Solutions	<ul style="list-style-type: none">• Vulnerability and Threat Prioritization• Attack surface validation and verification• Attack monitoring and early warning of Threats• Continuous and relative risk scoring



How is it different?

RiskSense is the only SaaS cyber risk management tool that provides a real time prioritization that combines the network, application, database and IoT layers.

- *This is the first cyber management tool that allows organizations to view their growing attack surface on a single pane of glass. From senior management to IT staff managing remediation tasks on a daily basis, the RiskSense platform streamlines and focuses cyber resources and investments, **enabling a proactive and preventative cyber security posture.***
- *This gives your organization an overall picture of the real time risk posture and helps prioritize remediation.*

What is the value to you?

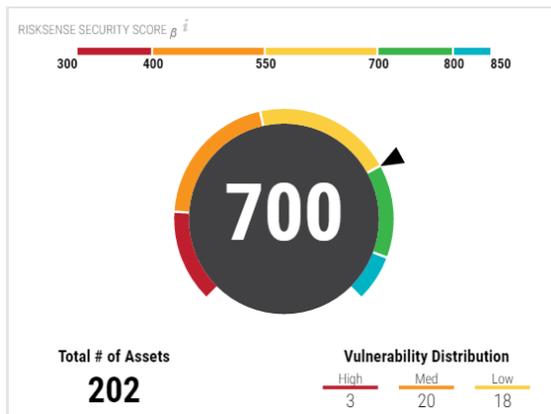
1. **Increases organizational cyber risk management capabilities:** RiskSense augments current cyber security tools and resources by ingesting scan data and correlating it with factors including business-criticality and **threat intelligence unique to RiskSense and garnered from over 100 intelligence sources.** Using the RiskSense platform can decrease the overall attack surface by



An NMLEA STAR Product

50% and security/IT teams greatly reduce the time to identify and analyze vulnerabilities and manage remediation actions by 90%.

2. **Supports enterprise-scale effectiveness:** The RiskSense platform provides an easily understood and communicated “RS3” credit type score improving internal communication and coordination while also prioritizing the highest risk vulnerabilities for IT Security teams that are dealing with an enterprise-scale attack surface.



RiskSense focuses on those vulnerabilities which have exploits/malware targeting them; that also have remote code execution (a key indicator of a dangerous risk); and finally, those vulnerabilities which are currently showing activity via our nationally recognized threat intelligence. This higher level and more strategic risk prioritization is continually proven far more valuable for a more threat-centric and expedited approach to the remediation process, than the more static CVSS based scoring.

3. **RiskSense integrates easily into sophisticated IT Security stacks:**

Our SaaS platform is designed to align with current and planned IT security architectures. RiskSense is designed to ingest data from a variety of scanner sources - network, application, IoT, etc. - then aggregate, correlate, and normalize all findings. This means that our customers can change their scanners to always use "best of breed" or use multiple scanners to further increase accuracy. Either way, RiskSense maintains the continuity of the program and focuses the program on risk and driving it out of the program.

RiskSense developed our platform to dynamically deliver pen test results via the platform. This means “Continuous Red Teams” can upload their own results to further enrich the overall vulnerability visibility. In addition, we integrate with the well know ticketing systems like ServiceNow, Jira, etc. For more information <https://risksense.com/resources/quick-videos/>

Learn more with a no-obligation 45-minute demonstration of the platform at work. Better yet, arrange for a no-cost “proof of value,” where you can use the platform in your environment, in your organization, and see for yourself how it can save you time, money and accelerate.

Contact us for a Cyber Risk Assessment or “Proof of Value” no-cost trial

For more information: cbcq@risksense.com | 401.524.7818 | <http://www.cbcgroupwins.com/risksense/>
Or, you can contact the NMLEA staff at cyber@nmlea.org.