



# Onyxia Enables Critical Infrastructure Leader to Leverage Data Intelligence to Strengthen Their Security Program and Reduce Risk Exposure



**I have lots of static tools for risk assessment.  
What I like about Onyxia is that it's continuous and ongoing.  
It gives us focus and discipline day-to-day.**

**- CISO of our Critical Infrastructure Client**

## About the Client:

Our client is a major Port Authority serving two states across air, land, rail and sea. The organization moves millions of people, services 1,500 square miles, and support billions of dollars in economic activity. They have been running for over 100 years and have nearly 7,000 employees.

The Port Authority specializes in designing, engineering, and operating the transportation infrastructure that moves people and goods to, from, and throughout one of the most economically competitive and culturally vibrant regions in the world.

## The Challenge:

Before Onyxia, our client's security team spent 160+ team hours pulling reports from numerous disconnected security tools. This was not only an inefficient use of their team's time, but the inaccuracy from 'point in time' results left them more prone to lagging risk management and wasted budget. Manually pulling their program data from disparate resources also left them with no central source of truth for the efficiency and performance of their security stack.

Furthermore, in light of the lack of unified, real-time data, they struggled to prepare critical board reports and effectively communicate the business outcomes of the cybersecurity program at the executive level.

### How Onyxia Helps:

With Onyxia, our client now has a central location to manage and report on the performance of their entire security program, allowing them to focus more time on program optimization and risk reduction.

Onyxia collects and analyzes data from our client’s entire security ecosystem with our data fabric. Based on the analysis, we provide our client with continual program assessment and benchmarking as well as meaningful insights regarding their security stack coverage and compliance efforts. We enable our client to leverage all the data they have from so many different data sources in one core management dashboard.

Their security program management now benefits from the following main improvements:

### Automated Program Measurement & Benchmarking

After onboarding Onyxia, our client was able to quickly move from manual spreadsheets to a fully customized program performance dashboard. They integrated their entire security stack via APIs and were able to see the raw data turn into actionable intelligence within an hour.



Our client was able to instantly select how they wanted to measure the effectiveness of their cybersecurity program by selecting the Cybersecurity Performance Indicators (CPIs) from our CPI library that were particularly relevant to them. The CPIs align with Onyxia’s custom security framework, addressing domains including Detection & Response, Vulnerability Management, Training and Awareness, Cloud Security, Identity & Access Management, Network Security, Device Management, and Mail & Web Security. We allowed them to connect multiple resources per CPI, see the exact formula used to measure the CPI and adjust the SLA according to their program needs and requirements.

Charts and graphs only tell part of the story, so we also give our client an easy way to contextualize their data with labeling. Custom labels allow our client to add

text to any point on a CPI chart. This helps them reference a change in performance by marking the event with specific information (i.e.- headcount change, new process or product, etc.).

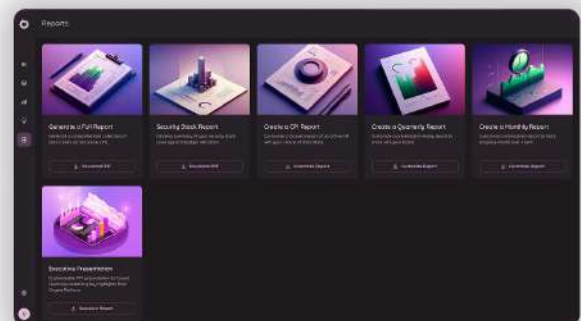
When it comes to program assessment, one of the features our client finds most valuable is the ability to benchmark their performance against the average SLA in different industries. This allows them to compare their performance to more highly regulated industries and increase the security measures of their program accordingly.

A key benefit of the assessment and benchmarking features we provide is the ability to not only understand performance in real-time but also over time. Our platform gives our client important historical CPI performance and benchmarking performance data over the past year.

## Streamlined Board Reporting

Whereas our client previously scrambled days before a meeting to compile and build their own board reports from scratch, with Onyxia, they can now download a variety of reports, including a customizable Executive Board Presentation, in a matter of clicks.

In addition to the customizable board presentation, our client also enjoys the ability to download CPI-specific reports, full reports with data trends across all active CPIs, quarterly reports, and monthly reports. Onyxia also provides a Security Stack Map report, which includes a detailed summary of their security stack coverage and budget allocation.



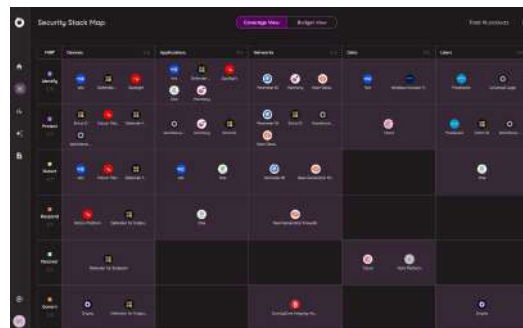
The value of these reports goes beyond the time saving and enables our client to effectively communicate to their stakeholders for better buy-in on their security initiatives and validate the investments in their program.

## Full Security Stack and Asset Coverage Visibility

Along with providing our client with an understanding of how their program is performing in relation to their goals and CPIs, we also leverage the data to help our client maximize the capabilities of their security stack.

The Security Stack Map, which was automatically generated as soon as our client integrated Onyxia with their environment, charts their security stack to a compliance-aligned coverage map, enabling them to optimize tech stack efficiency, identify gaps or overlaps in security stack investments, and ensure alignment with key frameworks.

The Security Stack Map also includes a Budget View, which provides our client with an intuitive investment heatmap detailing cost areas and highlighting where stack investments are allocated, allowing them to better invest their security budget.



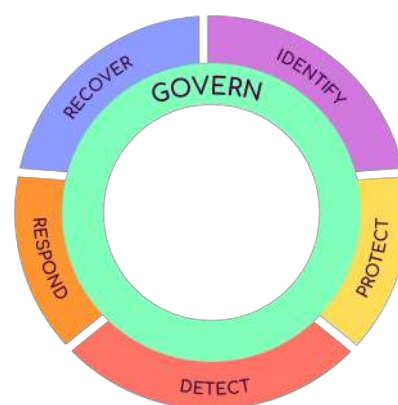
Additionally, from the data gathered on their environment, our client can compare their security tool coverage on specific assets. They can easily measure and compare security tool coverage across all the devices in their environment to ensure that there are no gaps or overlaps.



## Achieving Compliance and Aligning with Security Frameworks

Our client follows the new NIST 2.0 cybersecurity framework with the new 'Govern' function. We enable them to more easily achieve compliance and align with NIST 2.0 with two key features: our high-level dashboard and mapping of the security stack.

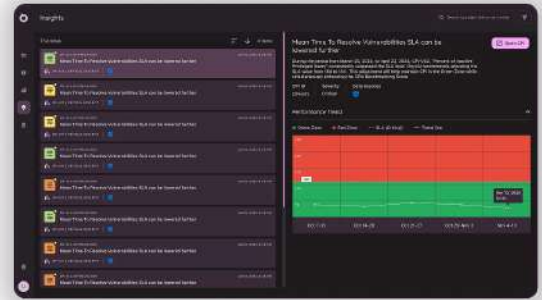
At the click of a button, our client can globally transform Onyxia's Cybersecurity Management Platform to a NIST CSF 2.0 aligned dashboard. The parent security categories and the Cybersecurity Performance Indicators (CPIs) align to match the NIST compliance framework.



With Onyxia's Custom Frameworks feature, our client can also quickly align their dashboard and Security Stack Map to custom-built frameworks, such as the Transportation Systems Sector (TSS) framework and SOC 2.

## OnyxAI: Proactive Program Improvements with Predictive Security Insights

With OnyxAI, Onyxia's AI Cybersecurity Predictive Management Engine, our client receives powerful insights that enable them to proactively optimize security performance, resource allocation and exposure management. They can quickly identify how to optimize their SLAs, which CPIs have data trend improvements or reductions, and which assets and/or framework domains are missing coverage.



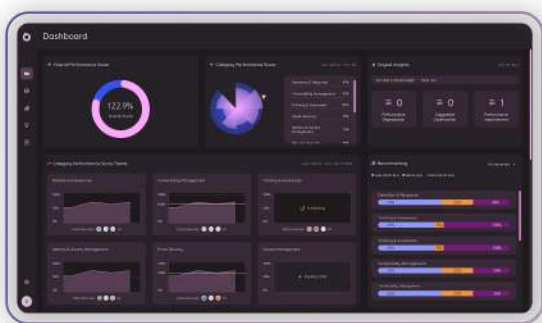
OnyxAI uses statistical analysis, machine learning algorithms, and NLP models to analyze data gathered from the organization's entire security ecosystem. With the integration of OnyxAI, Onyxia's Preemptive Cyber Defense & Planning Platform helps our client receive suggestions on how to improve security program performance, identify overlaps and redundancies in their security stack, and gain program trend predictions. For each CPI, they are able to see predictive performance analytics for the upcoming month.

The actionable and predictive insights from OnyxAI have allowed our client to quickly uncover critical security gaps, like administrator accounts lacking MFA, enabling them to preemptively reduce risk exposure and prevent future crises.

# Conclusion

Our client chose Onyxia's **Preemptive Cyber Defense & Planning Platform** over the competition because we provide them with a complete solution to manage, measure and optimize their security program. Moreover, with our Security Stack Map and Asset Coverage Analyzer, we enable them to easily map their security stack to their target cybersecurity framework, in this case, NIST 2.0, and compare security stack coverage across all organizational assets. This enables our client to achieve organizational compliance and maximize their security stack investment and efficiency.

Onyxia's offerings are especially significant in light of new regulations, like the SEC's cybersecurity disclosure rules, which require public companies to not only report material incidents within four days but also demonstrate risk management strategies and efforts over the past year. Moreover, the new rules have encouraged organizations to ensure they have an individual with cybersecurity expertise reporting to the board on the business-level impact of cybersecurity measures.



In short, we provide complete program management, giving CISOs and security leaders the takeaways they need to continually strengthen their security program performance and proactively improve their exposure management measures.