Onyxia

Onyxia Enables Manufacturing Leader to Fully Leverage Data Intelligence to Strengthen Their Security Program and Risk Management Efforts

Onyxia puts us in a much better position to assess our security program and exposures. With Onyxia, we are able to save at least 160 working hours a month that one full-time analyst would traditionally spend on manual reporting and instead, focus more time on our actual risk management strategy.

- CISO of our Manufacturing Client

About the Client:

Our client is a publicly-traded company with over 40,000 internationally-based employees and multiple subsidiaries. They are a world-class provider of passive components services with capabilities on a global scale, including production and sales facilities in Asia, Europe, and the Americas.

Their offerings target key vertical markets, including mobile, tablet PC, industrial/power, alternative energy, medical and automotive applications. They serve diversified leading global customers, such as EMS, ODM, OEM, and distributors.

The Challenge:

Before Onyxia, our client's team spent hours pulling reports from dozens of 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.

Moreover, with the inefficiency in achieving a cohesive and streamlined way to manage and optimize their entire cybersecurity program, they also struggled to unify their global security strategy across their portfolio of companies and align their program with new regulation requirements, like the SEC's cybersecurity disclosure rules.

How Onyxia Helps:

With Onyxia, our client now has a central location to manage 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, and Device Management. 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 had to compile and build their own board reports from scratch, with Onyxia, they can now download a PDF report of all the CPIs or easily create a more focused report that includes the specific CPIs relevant to the board.

Instead of doing this manually, they can now receive a board-ready report in one click. This report includes a table of contents, a granular look at all the CPIs, contextualized performance labels, the definition of and business value of the metric, and the performance over time. In addition to the full and focused reports, Onyxia has two additional preset reports with monthly and quarterly options conveniently ready with one click.

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

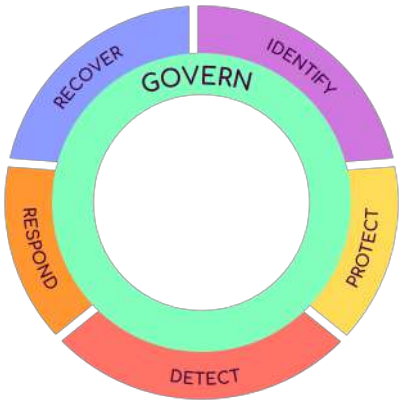
Along with providing our client with an understanding of how their program is performing in relation to their goals and CPIs, we also leverage the data to help our client maximize the capabilities of their security stack.

The Security Stack Map, which was generated automatically as soon our client integrated Onyxia with their existing environment, now enables our client to optimize tech stack efficiency, identify gaps or overlaps in security stack investments, and ensure alignment with key frameworks.

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) can be set to match the NIST compliance framework.

At the same time, our Security Stack Map automatically adds each new product integration our client sets up in their dashboard. Those products get charted into cells based on their associated asset type category (Devices, Applications, Networks, Data, and Users) and NIST 2.0 pillars (Identify, Protect, Detect, Respond, Recover, and Govern).

OnyxAI: Proactive Program Improvements with Predictive Security Insights

With OnyxAI, Onyxia's AI Cybersecurity Predictive Management Engine, our client will receive powerful insights that enable them to proactively optimize security performance, resource allocation and risk management.

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 Cybersecurity Management Platform will help our client identify overlaps and redundancies in their security stack, receive suggestions on how to improve security program performance, and gain program trend predictions that could reduce risk and prevent future crises.

Conclusion

Our client chose Onyxia over the competition because we provide them with a **complete solution** to measure, manage, and optimize their security program. Moreover, with our Security Stack Map and Asset Coverage Analyzer, we enable them it 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 risk management measures.