CASE STUDY

BTB Security delivers high-quality third party risk assessments in less time with Whistic

BTB SECURITY + whistic

Introduction

BTB Security, a boutique managed service and security consulting firm that helps businesses improve their cyber security posture, needed a way to more efficiently conduct third party risk assessments on behalf of its clients. The processes in use were manual and time consuming and the team knew there had to be a better way.

When David Menichello, Director of Advisory at BTB, began looking for an enabling solution for the third party risk assessment process, he wanted something that would speed up the process without affecting the quality of the service his team delivered.

BTB ultimately decided Whistic was the best fit for them. The following is a conversation with Menichello that delves into the reasons why BTB chose Whistic and how it's helped improve the service delivered to its clients.

“Being able to leverage existing security info in the Whistic Trust Catalog. That’s helped get us to some answers sooner than it was before Whistic.”

David Menichello, Director of Advisory Services at BTB

Conversation

David Menichello, Director of Advisory Services at BTB

Whistic: First off, why don't you describe BTB Security for us and what your role is there.

David Menichello: BTB has been around since 2006. We're a boutique infosec company. Our main lines of business are assessments—penetration tests, threat and vulnerability, governance, webapp —things like that. We have a managed detection and response service, RADAR®, where we use our technology to monitor client environments 24 x 7 and neutralize threats on their behalf.

We also have CISO Advisory, which is a strategy practice where we design, implement, and run security programs for our clients that are aligned with their business goals and commensurate with their risks. That's where third party risk management comes into play for our clients.

Whistic: What is your role at BTB?

DM: I'm the Director of Advisory, so I oversee any of the consulting work that we do, including offensive security, threat assessments, and the CISO Advisory practice.

Whistic: Are you using Whistic for just VRM or VRM and Profile?

DM: The mainstay of what we do is perform third party security assessments on behalf of our clients, so VRM is the primary Whistic module in use. VRM gives us a centralized platform for administering, tracking, and reporting on assessments we execute.

Whistic: Prior to Whistic, how was your process for sending out questionnaires and assessing the vendors once you receive it back different?

DM: It was a mixed bag. We would leverage industry standard security questionnaires that we would administer to the third parties we were assessing (or accept ones that were already completed, provided they were up to date). However, it was a highly manual process; very much email based with a lack of centralized data and reporting. Overall it was clunky.

As our client base grew, and subsequently our number of assessments, we knew that to continue to produce high quality work and get to the heart of the security shortcomings that could materially impact our clients, we'd need a purpose-built enabling technology. Our legacy process was not sustainable.

Whistic: Prior to Whistic, do you have an idea of how long it would take to conduct an assessment from collecting the vendor information to completing the assessment?

DM: Generally, a couple of weeks. I would say the shorter ones had a turnaround time of one to two weeks. The longer ones were more in the four-to-six week range. We've seen that come down a bit as well as being able to leverage existing security info in the Whistic Trust Catalog. That's helped get us to answers sooner than before.

Whistic: What was the biggest pain or problem you were seeing that led you to look for a solution like Whistic?

DM: Two things. One, with us being in consulting and performing this as a service for our clients, I needed something that clients saw as a net gain for them. A service that had all the elements of a well-designed TPRM process that could be performed for them in a cost-effective way. Two, in order to scale and bring this service to clients in a cost-effective manner, I had to make our CISO Advisory team more efficient. In other words, maximize our throughput, enhance our quality, and drive down operating costs. Whistic helps make our offering enterprise grade through consistency, scalability,, and efficiency associated with the workflows and centralized reporting that are native to the system.

Whistic: Did you evaluate any other solutions that were similar to Whistic?

DM: We did. We evaluated one other platform and ultimately ended up deciding on Whistic.

Whistic: What was it about Whistic that made you choose us over the competition?

DM: Two main reasons. First, it was going to lower the cost to perform assessments. And second, it gave us the ability to white label the solution. Each client has a dedicated instance. Their portal and reports are customized with their branding, such as logos and colorways. On the back-end, it's very convenient for our consultants to be able to securely authenticate once and then toggle between different client portals. Lastly, this acquisition model was simpler than the other solution we evaluated. With Whistic I purchase a bank of annual assessments that I forecast we'll need and then allocate them across my clients. And if I need to buy more, I can. The other solution would have meant BTB needing to be a reseller, which is time-consuming, more complex, and introduces added management overhead.

Whistic: What's been the biggest benefit you've seen since implementing Whistic?

DM: In the short term, it's been the ability to organize our work easily. We have one central place to go even though we're toggling between client instances, it's all right there. It's familiar, easy to navigate, and enables the team to work through their assessments and reports quicker.

Longer term as we start to compile an even larger population of completed reviews, it's going to be the ability to have better, centralized reporting and structured data that we can interrogate. Previously, we were data rich and information

poor, so to speak. With Whistic, we'll be able to start extracting the business intelligence out of the data that we've amassed.

Whistic: What type of business intelligence are you looking to glean?

DM: It can be a struggle to ensure the vendors we assess are in compliance with their contractual obligations. We need to have the ability to tag certain controls as key and hone in on the things that are really material for our clients' businesses, and operations and reputational risk. As we learn more, we'll really be able to drill down in the areas that truly impact security, while also getting a broad-based glimpse of what their security program looks like.

Whistic: Can you cite any specific examples of where Whistic has helped your clients?

DM: Yes, we got an immediate improvement in our ability to efficiently and professionally report quarterly metrics to our clients. Reporting is very important to demonstrate the value we're providing to clients, and Whistic has improved our ability to do that.

Whistic: Could you quantify the impact that Whistic has had on your business or clients?

DM: It's definitely made us more efficient. It's made the team's day-to-day a bit easier. Since embedding and basing our processes off of [Whistic] and certainly with outside factors of clients coming to us and saying, "I've got to manage outsourced risk because of SolarWinds or Kasaya or other things," our ability to prospect and gain interest in our service has gone up. It's helped us show prospects that we're not just doing this in an ad hoc manner. There really is a comprehensive, software-backed process that they can leverage and benefit from.

Whistic: Final question. You mentioned that in the future you were wanting to build out more reporting. What are your other future plans for Whistic?

DM: A lot of that will be dictated by what common standards get adopted. Whether it's GDPR or GDPR Lite, privacy standards or the CMMC standard within the federal space or complying with the requirements around CUI, it really depends on what's germane to our clients' businesses and what standards prevail and what questionnaires within Whistic that we can leverage based on that standard. I think that the nice thing about the platform is that we have so many different question sets that are supported and that there's some forethought into what's coming down the road that we might need to prepare for and not be in reactive mode.

Results

Simplified the vendor assessment process

"[Whistic has] made us more efficient. It's made the team's day-to-day a bit easier." — David Menichello, Director of Advisory Services at BTB

Enabled faster vendor assessments

The team at BTB now delivers the same quality of work it's known for in less time.

Centralized and organized vendor assessment data

Instead of dealing with spreadsheets and emails, BTB manages the entire vendor assessment process inside of Whistic.

www.whistic.com