CASE STUDY: CISA CYBER+INFRASTRUCTURE

ANALYST1

A STEP ABOVE: WHY ANALYST1 IS CISA'S THREAT INTELLIGENCE PLATFORM OF CHOICE

DESCRIPTION

In 2017, CISA was on the hunt for a more efficient threat intelligence platform. After careful comparison and analysis of over 50 vendors, they landed on Analyst1. With Analyst1, CISA was able to drastically cut back on time spent aggregating and correlating threat data so they could focus more on doing real cyber threat analysis.

In 2017, CISA lacked the ability to process threat intelligence reports in an automated fashion. We had the pleasure of speaking with Omar Cruz, Project Manager for CISA, to uncover how the organization was able to increase efficiency by employingAnalyst1 as their new threat intelligence platform.

> We were processing hundreds of intelligence reports manually, and it took one analyst approximately eight hours to process one intelligence report.
>
> — Omar Cruz, Project Manager for CISA

THE PROBLEM

The biggest pain point for CISA was that they were doing all of their information processing manually. It was taking one analyst several hours to get through one intelligence report. Then, these analysts had to determine how to use the data, manually dissect it, connect the dots from dozens of other vendor reports on similar issues and attempt to identify the threat. This extremely tedious and manual process was very time-consuming for the analysts. So, CISA sought out a solution that delivered intuitive automation.

MARKET RESEARCH

As the number of threat intelligence reports being shared with CISA increased, the organization decided to shop around for a commercial threat intelligence platform that would bring automation into its threat intelligence process using a three-phase approach.

PHASE 1 REQUIREMENTS GATHERING

The first phase of market research involved sitting down and talking with internal analysts to determine what exactly they needed. CISA collected hundreds of requirements from these interviews before moving on to Phase 2.

PHASE 2 DOWN-SELECT PHASE

Once the list of requirements was gathered, CISA listed a bid to the public, to which over 50 vendors replied. To narrow down the candidates, CISA developed a scoring system to determine which vendors either met or did not meet the analyst's requirements. The top three vendors moved on to Phase 3. Analyst1 was one of them.

PHASE 3 BAKE-OFF

Analyst1 and the other two finalists were then put to the test in a lab environment. CISA brought in 10 analysts from different teams to interact with each tool. Over a span of 30 days, the analysts tested the tools and determined which of the three met the majority of their requirements. Analyst1 was declared the winner in July 2017.

EMPLOYING ANALYST1

After two to three months of procurement, it was time to put Analyst1 to work. In October 2017, CISA instituted a Limited Operational Capability test for 20 to 30 analysts to go about their daily operations using the platform and identify any hiccups. A few necessary modifications were pointed out, and Analyst1 implemented the changes to accommodate the new requirements.

WHY ANALYST1?

A few things helped Analyst1 stand out from the other vendors CISA was considering:

- The solution met the majority of CISA technical requirements. Many of the other vendors were not able to automatically enrich the information.
- Analyst1 promised more intuitive automation. CISA was highly impressed with the platform's ability to correlate data from dozens of other sources in a matter of minutes.
- It offered next-level data enrichment. CISA wanted to ensure that all of their data would be enriched with additional context so they could better discern what is going on when looking at countless reports.

> Now that Analyst1 is doing all that [work] for us up front, we're freed to then focus on doing real cyber threat intelligence analysis, really connecting the dots. Now we can actually paint a much better picture. ... By having better analytics, we can do a much better job of reporting and assessment of what the adversary is doing.
>
> — Omar Cruz, Project Manager for CISA

WHAT'S NEXT?

CISA seeks continued innovation with their threat intelligence, and Analyst1 aims to provide it to them. On their list of improvements is a chat feature for better collaboration between analysts and a revamped search feature so that teams can be aligned no matter the use case.