SUMMARY

MS-ISAC® sought to revamp its internal threat intelligence capabilities to better collect, analyze, and provide relevant information to members. Analyst1 provides an efficient, straightforward solution that puts the MS-ISAC’s analytic expertise front and center.

The MS-ISAC’s critical defense mission, combined with unique member needs, required the MS-ISAC to pursue a threat intelligence platform with full control over the data and how it is used. To support key elements of its defense-in-depth strategy, the platform must also integrate with current and future technologies in addition to meeting other key requirements.

The new solution had to easily facilitate timely and relevant intelligence sharing at scale in multiple formats without passing cost to members. After a thorough evaluation process, the MS-ISAC selected Analyst1 as its platform. Analyst1 allows internal MS-ISAC team members to manage evidence collection, conduct analysis and correlation, prioritize intelligence sharing, and track malicious actors and campaigns in real time.

KEY DECIDING FACTORS

1. Control over the actual data. Analyst1 resides in MS-ISAC’s operational environment, putting the MS-ISAC in control of what goes in, what stays in, and what goes out to members. Members have limited resources to conduct their own analysis, instead relying on the MS-ISAC’s resident expertise and unique perspective to drive what threats should be prioritized for action. Members require low volume, high fidelity feeds, and Analyst1 allows the MS-ISAC to provide that by keeping the control of the database local. Analyst1’s automation and data organization capabilities allow the feeds to be populated in near real-time, increasing the team's efficiency and the platform’s overall effectiveness.

2. Ease of integration with other capabilities. Analyst1’s interface makes managing hundreds of inbound sources easy and outbound sharing clear. Analyst1 can integrate with any capability that can import and export data in a variety of standard formats.

3. Straightforward system management. Analyst1 allows modifications to settings to improve scalability, automation, and rule creation. It is critical for the MS-ISAC to have a platform flexible enough to evolve with the threat environment.

RESULTS

Adoption of Analyst1 has led to significant improvements in a short time span for MS-ISAC, including:

- Higher reliability in the quality of data shared (i.e., far fewer false positives)
- Ability to quickly assess the value of evidence coming in and data going out
- Higher efficiency through the use of a "single pane of glass" for intelligence collection, analysis, and sharing, resulting in better information out to members faster

For more information about Analyst1, check out our site or contact us and a representative will reach out and help answer any questions you may have. You can also request a demo if you’d like to see our platform in action.

ANALYST1