CASE STUDY

IMPLEMENTATION OF SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE SOLUTION FOR VISTARA

About the Customer

Vistara, a joint venture between Tata Sons Private Limited and Singapore Airlines Limited (SIA), started its operations in India in 2015, blending Tata’s historic service excellence with SIA’s global aviation experience.

Vistara has flown more than 20 million flyers across 36 destinations in just five years of operations and is aggressively expanding its operations across the globe. The airline became the first to operate the Boeing 787-9 Dreamliner aircraft in India. Vistara is highly ranked on Trip Advisor and has been the winner of multiple ‘Best Airline’ awards since operation.

36 Destinations

20 mn Passengers

05 years in 24x7 operations

www.tataadvancedsystems.com
Business Challenge:

Since inception, TATA SIA airlines limited (Vistara) is regarded as a security-focused organization. Vistara continually looks to optimize and fortify its guard against modern cyber threats. The organisation has a clear intention to stay "ahead of the curve"

With broad range of security solutions implemented across hybrid and multi-cloud infrastructure and thriving the helm of air transportation, there was a need to augment the manpower with automation and orchestration. Further attackers today are utilising novel ways to fulfil their malicious intentions and thus it becomes imperative for analysts to get a breathing space and focus on high fidelity alerts.

To address this requirement, Vistara aimed at automating repetitive tasks and thus allowing analysts to focus on high fidelity alerts. A clear answer to this was a Security Orchestration, Automation and Response solution, selection of which also depends on current infra and forward integrations available with the solution.

Solution Implemented:

As a trusted security partner to the airline we diligently evaluated multiple SOAR solutions while selecting the perfect fit for the infrastructure at Vistara. The solution thus implemented covered >90 percent infrastructure at the airline.

Automation is the key to optimising repetitive tasks which needs little to no human intervention. The same follows for responding to threats like blocking a categorised malicious IP, isolating an infected endpoint, or blocking a suspicious account activity attempting to brute force or escalating privileges.

The SOAR (Security Orchestration Automation and Response) solution layered over the existing SOC platform and was deployed on cloud. It helped the airline to reduce alert fatigue to SOC analysts, remove false positives, automate repetitive tasks, and respond to threats proactively.

Apart from deployment, standard managed security services were also provided to help create clear playbooks, ingest threat intelligence/analytics and aid threat hunting.
Benefits:

- Average of 3.5 hours in a day per analyst saved, since inception
- Covered 5000 users across destinations
- Average 11 days per month saved per analyst to focus on high fidelity alerts
- 08 weeks of manual effort saved, since inception
- Oversight on 300+ multi-cloud infra
- More than 80 device actions automated
- More than 25 response automated
- Enrichment from more than 40 global threat feeds

“With constantly evolving adversary Tools, Techniques and Procedures (TTPs), adopting combination of human and machine power fortified Vistara to thwart evolving tactics through automated actions. SOAR allowed us to build digital orchestration to define incident analysis and response procedures thereby aiding our threat intelligence and automation capabilities in neutralizing threat actors.”

Subhash Kumar Mishra
Head IT enterprise, TATA SIA Airlines Limited – Vistara

www.tataadvancedsystems.com