binalyze!

Turkish Airlines counts on Binalyze AIR to build a remote incident response program

Challenges

Turkish Airlines required a forensic investigation solution to collect, analyze and investigate digital forensic evidence remotely and at scale from across their global network. This would allow them to achieve their goal of remediating cyber incidents in a fast and efficient manner.

Turkish Airlines is a globally recognised aviation giant with operations in 129 countries, 330 cities and 340 airports. They employ over 40,000 people worldwide.

As a member of IATA, Turkish Airlines is integrated with the global aviation network and relies on a complex infrastructure of critical business and supply chain systems. Protecting these systems, individually and collectively, is a top priority for their security team.

This requires a thorough and constant cyber assessment across all stakeholders including aircraft and equipment manufacturers, air-traffic control, airports, airlines and all the other components of the aviation supply chain.

In addition to this supply chain complexity, airlines naturally operate in a highly distributed manner with operations in hundreds of different countries and cities. Each individual location has its own IT requirements and infrastructure.

Aviation is one of the most distributed industries in the world. The requirement to interface with public and private cloud services further distributes the potential attack surface that must be secured.

A surge in global travel over recent years, combined with digital transformation initiatives and increased connectivity, has delivered many benefits. However, those benefits have come with an increased complexity that poses additional challenges in terms of cybersecurity.

The increasing need for integration and automation at the business level necessitates more robust and resilient protection of IT and network infrastructure to ensure business continuity in a highly regulated industry. All security policies must satisfy a high standard and align with safety-first objectives.

In response to the complex and challenging environment, Turkish Airlines has invested heavily in cybersecurity. The Turkish Airlines Cyber Defense Center (CDC) continues to build a world-class team of talented security professionals and utilise best-in-class technology solutions including EDR, SIEM and SOAR solutions.

The company also pays close attention to the latest innovations and technological improvements to ensure they maintain a high degree of cybersecurity readiness and constantly expand coverage and capabilities through the early adoption of new security tools. This policy helps to maintain a strong security posture.

Customer
Turkish Airlines

Industry
Aviation

Region
129 countries globally

Founded
1933

Employees
40,000+ Worldwide

Success Highlights:

- **Decreased investigation times** from weeks to minutes
- **Decreased dwell time** to collect and analyze forensic data
- **300% improvement** in evidence collection speed
- **55% faster** average incident response time

Adopting Binalyze AIR for Efficiency and Collaboration

With operations across 4 continents, investigations involve endpoint assets distributed all over the world.

Security operations are carried out from a central CDC located at the global headquarters in Istanbul. Previously, it was extremely time consuming and expensive to travel to the endpoint assets under investigation and collect forensic evidence.

This was a key motivation to invest in a Enterprise Forensics solution like Binalyze AIR to remotely collect evidence from any endpoint in just a few minutes.

"As part of our security operations program, we run regular cybersecurity exercises. In one of the exercises we have done before implementing Binalyze AIR, we tried to investigate suspicious endpoints in Afghanistan. It took us more than a week to bring the endpoints into the CDC for investigation.

During that process we were also dependent on staff on site, who do not have cybersecurity and IT skills, to prepare and pack the devices appropriately enough for us to be able work on them.

We have repeated the same cyber security exercise after implementing Binalyze AIR to our infrastructure and it took less than 1 hour to remotely collect evidence from the endpoints in Afghanistan, investigate the incident, do the reporting and close the case.

We also had no issues with human errors during the evidence acquisition process, since the whole process was done by Binalyze AIR remotely and automatically." said Kadir Yıldız, SVP, Turkish Airlines.

Reducing dwell time and speeding up incident response

The remote and fast evidence acquisition and triage capabilities of Binalyze AIR, in addition to its automation and native integrations with other security systems, helped the Turkish Airlines team accelerate the incident response process by 55%. This also had the effect of reducing the overall dwell time for cyber incidents.

With Binalyze AIR the Turkish Airlines CDC team are able to collaboratively work on the same case from a single pane of glass. Granular role definition and access control ensures that this collaboration is done with appropriate permissions profiles for each individual team member.

With Binalyze AIR, average case resolution time dropped from 3 weeks to 1 hour bringing the case backlog under control. The overall efficiency of the incident response team has increased significantly with Binalyze AIR.

"In a distributed environment like Turkish Airlines, it is hard to get the full granular visibility and root cause of incidents at speed and scale. **With Binalyze AIR's remote evidence acquisition and automated triage we can now investigate and close a case under 1 hour.** This would normally take more than 3 weeks in the past." said Kadir Yıldız, SVP, Turkish Airlines.

Conclusion

With Binalyze AIR, Turkish Airlines can now collect, analyze and collaboratively investigate more than 280 evidence types from endpoint assets across the globe remotely, which has significantly reduced the time and resources required previously.

Turkish Airlines have been able to achieve their objective of remediating cyber incidents faster and more comprehensively with Binalyze AIR. This has dramatically reduced the average investigation time allowing them to close cases in hours instead of weeks.