binalyze!

TURKCELL

Turkcell counts on **Binalyze AIR** to build a resilient incident response program

Challenges

Turkcell needed an effective digital forensics and incident response platform to help incident response teams quickly and precisely collect, investigate and analyze evidence, carry out compromise assessment, complete the reporting and take necessary remediation actions on time.

Challenges in cybersecurity forensics

Turkcell is a converged telecommunications and technology services provider founded and headquartered in Turkey.

They serve their customers with voice, data, TV, digital security services, and value-added consumer and enterprise services on mobile and fixed networks.

In addition to 50 million subscribers and operations in 5 countries, Turkcell provides managed services to corporate customers.

Cutting through the noise of overflowing data.

Turkcell is a large enterprise with more than 20,000 employees across the globe. The shift from office to remote-working during the pandemic accelerated the rapid increase in data volume, and number of data sources, which has increased the noise that the Cyber Defence Center (CDC) is required to cut through in recent years.

This issue has been amplified by the advanced cyber security threats specifically focusing on telcos as a high-value target.

From over 550 data sources, Turkcell's CDC processes eight billion raw data logs every day. Using sophisticated data correlation processes, these are filtered down to 400 million logs of significance which results in over 300 daily alerts that need to be handled by their experienced security teams.

Combining these factors with strict data privacy regulations such as KVKK (Turkish Data Protection Act) and GDPR has left Turkcell's CDC in need of forensic and incident response solutions that bring cyber resilience to their security posture, decrease risk and ensure business continuity.

To support Turkcell's vision of building a cyber resilient environment, their team developed the BOZOK Cyber Threat Intelligence (CTI) platform, which includes data leakage, brand protection, and vulnerability modules.

Reducing exposure and risk to strengthen incident response.

"Efficiency is the most critical parameter in incident response processes in an era where cyber incidents become more widespread with remote working.

The risk associated with incidents threatens all corporate structures more and more every day," states Dr. Emin İslam Tatlı, Director of Cybersecurity at Turkcell.

Customer
Turckcell

Industry
Telecommunications

Region
Middle East, Turkey & Africa

Founded
1994

Employees
20,000+ Worldwide

Success Highlights:

- **Decreased evidence collection times from days to minutes**
- **Improved efficiency with remote evidence collection & automation**
- **Eliminated human errors in evidence collection**
- **49% FTE time and effort saved**

Additionally, GRC (Governance, Risk and Compliance) processes such as KVKK must be performed quickly and obligations arising from these regulations must be fulfilled.

Turkcell's key motivation when investing in Binalyze AIR was to enable such critical processes to be managed in the fastest and most accurate way.

Finding the "unknown unknowns" with Binalyze AIR.

At Turkcell, the incident response team's main task is to collect and categorize the evidence and artifacts left behind by an incident to speed up its investigation and response processes.

It is crucial to discover all traces left by attackers to fully understand what has happened. **Binalyze AIR helps Turkcell to investigate over 280 artifact and evidence types in under 10 minutes. AIR provides a central hub for analysts to collaborate and work on the same case from a single interface remotely.**

Speed and accuracy are the key necessities of the team to highlight unusual or suspicious activities and identify the "unknown unknowns" to shorten the time to contain and remediate.

Additionally, the ability to remotely manage the network assets and take automatic actions after an alert allows the team to be more agile and helps them leave noun attended traces or devices behind.

Binalyze AIR gives the Turkcell team granular visibility on the incident and helps them to start their analysis efficiently with snapshots that highlight the differences before and after an incident.

With Binalyze AIR's ability to collect evidence instantly and remotely, the need to physically travel to the endpoint's location to collect evidence from remote endpoints has been eliminated. The process of collecting evidence, which used to take days, has now been reduced to just minutes.

"Binalyze AIR's easy to use interface helped our analysts to quickly adapt, prioritize and start conducting incident analysis which minimized the time needed for education and onboarding.

Even the less experienced analyst can start using Binalyze in a few hours. With Binalyze, we know where to start our investigations. Binalyze is the only solution that addresses this challenge."

– Dr. Emin İslam Tatlı

"Turkcell's forensic and incident response team saved approximately 49% of the human and time resources used, thanks to the comprehensive structure of Binalyze AIR" states Dr. Emin İslam Tatlı, "Binalyze AIR's easy to use interface helped our analysts to quickly adapt, prioritize and start conducting incident analysis which minimized the time needed for education and onboarding.

Even the less experienced analyst can start using Binalyze in a few hours. With Binalyze, we know where to start our investigations. Binalyze is the only solution that addresses this challenge."

DFIR for modern Incident Response Teams.

Binalyze AIR has features that go beyond traditional forensics solutions and provide convenience for modern, large enterprises like Turkcell.

The interACT remote shell feature of Binalyze AIR allowed the Turkcell team to directly query remote endpoints in a cross-platform remote shell session, all while maintaining a permissions-based user environment and comprehensive audit logging.

Enriched DRONE reports allowed the team to see suspicious events along with their scores and verdicts. This provides assisted compromise assessment and considerably simplifies the work of the SOC teams. It is now possible to respond instantly and with full accuracy to information requests sent by official institutions.

Conclusion

With Binalyze, Turkcell has been able to increase both efficiency and efficacy in their incident response processes. In addition to the end-to-end use of Binalyze AIR in analyzing cyber incidents, Turkcell plans to utilize the product's capabilities to discover and investigate potential cyber incidents that have not surfaced through threat hunting, providing a new level of cyber resiliency.

On the back of a successful deployment to their internal Cyber Defence Center systems, Turkcell is preparing to present Binalyze AIR to more than 90 MSSP customers to help them with fast evidence collection and analysis.