Delivering Incident Response Excellence: How Wipro Enhances Client Services with Binalyze AIR

Company overview

Wipro is a global leader in IT, consulting, and business process services, operating in over 50 countries with a workforce exceeding 220,000. Considered one of the select number of Big Tech organizations, the company has a rich history spanning 75 years, with decades in the IT industry.

Wipro provides comprehensive IT solutions across various industries, including delivering top-notch critical incident response and compromise assessment services in cybersecurity. A commitment to excellence and continuous improvement led Wipro to seek out Binalyze's Investigation and Response Automation Platform, AIR.

Challenges

- Time-consuming manual processes
- Limited scope of existing tools
- Responding to fast-moving attacks

Challenges in cybersecurity forensics

Wipro offers a wide range of IT security services, ranging from strategic consultation to dealing with active threats. Digital Forensics and Incident Response (DFIR) plays an important role in Wipro's security provision, especially as cyber threats have grown more aggressive and sophisticated.

David Charbel, Global Head of Next Gen Threat Hunting at Wipro, explains: "We're seeing more advanced attacks where threat actors are aiming to blend in with daily network activity and go undetected. It's essential that our customers are confident we can detect and respond to these attacks before they get out of hand."

Against this increasingly hostile threat landscape, the Wipro security team decided to review its capabilities and ensure it could continue to provide high-quality protection for its customers. One of the biggest priorities was the ability to identify and respond to fast-moving attacks before they could disrupt customer operations or access sensitive data.

"We found that many of our processes were too manual and involved too many different tools," David explained. "Previously, multiple tools were used to parse manually extracted data like hives, event logs, amcache, and so on. Bringing that into a single pane of glass with Binalyze AIR eliminated the need for multiple parsing workflows."

"This meant that critical steps like evidence acquisition could be too slow and disjointed. Working with a large number of diverse customer environments, efficiency is a top priority for us."

David continued: "As well as stopping attacks and limiting their damage, we're also seeing more demand for detailed post-incident forensics. We need to get to the core of why and how threat actors were able to do what they did in the environment, and customers are also under more pressure from regulators to determine how an incident occurred."

As Wipro sought to enhance its cybersecurity forensics and incident response capabilities and expand their service offerings, the need for a solution that offered faster, more automated evidence acquisition and analysis became clear. Further, with many organizations tightening their spending, the Wipro team needed to find a solution that would not result in increased costs for customers.

Customer
Wipro

Industry
IT, Consulting, and Business Process Services

Region
Global

Founded
1945

Employees
234,000

Website
www.wipro.com/cybersecurity/

Success Highlights:

- **Improved efficiency** and collaboration
- **Accelerated evidence acquisition** by up to 10x, from 24-48 hours to just 2-4 hours
- **Enabling triage** in as little as 1 hour
- **More time for high value,** consultative activity
- **Scaled to service a large pool** of international clients efficiently
- **Identified and resolved a long-term** web server compromise within 8 hours

Adopting Binalyze AIR for enhanced incident response

The team was able to move swiftly in bringing in a new solution to address its challenges, and David explains that Binalyze AIR was always their first choice.

AIR is a highly automated investigation and response platform designed to be both extremely fast and easy to use. The platform greatly accelerates investigation processes with its integrated compromise assessment capability, DRONE, capable of analyzing both acquired evidence and live systems. Findings are available through AIR's Investigation Hub to give the team a unified, 'single pane of glass' approach to investigating their cases.

'Using Binalyze AIR, we identified a web server that had been compromised for years. Within less than 8 hours, we assessed the full extent of the compromise, revealing multiple incidents and enabling swift remediation.'

David further explained: "We'd heard very positive word of mouth about AIR, so once we'd gone through a demonstration and tried it out, it was almost a foregone conclusion. We are afforded a lot of autonomy as experts in our field, so we were able to make the decision and bring in the best tool for the job quickly." Wipro chose Binalyze AIR for its advanced capabilities in remote evidence acquisition and automated analysis to accelerate the team's investigation and response capabilities. The selection process was driven by the need to address the inefficiencies and limitations of their existing tools and processes. Binalyze AIR's ability to quickly and comprehensively collect and analyze over 500 types of evidential artefacts was a game-changer, providing forensic-level visibility with context needed for comprehensive response and hunting.

David noted: "Binalyze AIR stood out because of its ability to handle large volumes of data quickly and accurately. The automation features, especially the timeline and triage, have transformed our approach to threat hunting and incident management."

Automation was one of the standout capabilities for Wipro as it drastically reduced the need for manual intervention. Implementing Binalyze AIR allowed the team to conduct rapid and efficient evidence collection remotely, which was previously a significant bottleneck in their process.

Binalyze AIR also enhanced collaboration within Wipro's cybersecurity team. The tool's unified interface provided a single point of visibility for all incident data, making it easier for analysts to work together on investigations using the Investigation Hub.

This collaborative environment was crucial for maintaining a high level of efficiency and effectiveness in managing cybersecurity incidents. The platform's role-based access control ensured team members could collaborate securely and effectively.

Finally, Binalyze's pricing structure and the low-resource nature of AIR meant that the Wipro team could improve its capabilities without any cost or IT resource burden for its customers.

A transformative result

Binalyze AIR has had a powerful impact on the team's workflows. David highlighted that it now served as one of their primary tools.

'The efficiency gains from Binalyze AIR have been remarkable. We can perform in-depth analyses and respond to incidents much faster, which has been crucial in maintaining the high standards of cybersecurity incident management our customers need.'

He explained: "The efficiency gains from Binalyze AIR have been remarkable. We can perform in-depth analyses and respond to incidents much faster, which has been crucial in maintaining the high standards of cybersecurity incident management our customers need. The remote evidence acquisition feature alone has saved us countless hours previously spent on manual processes."

One of the most notable outcomes was the dramatic reduction in time required for evidence collection and analysis. Before Binalyze, evidence acquisition could take 24-48 hours depending on client resources. Now, collection can be completed in just 2-4 hours, or less than an hour for triage for endpoints where Binalyze AIR is already deployed.

This allowed the team to conduct quicker triage and increase caseload capacity. The efficiency gain meant that Wipro could handle a higher volume of incidents without compromising on the quality of their investigations.

"This agility is really essential for us," David continued. "Cybersecurity is always unpredictable, and almost every week we're called in to help on an incident with a customer on an emergency basis. We need to be ready to jump into a crisis at any time."

The decision to integrate Binalyze AIR into Wipro's cybersecurity infrastructure was further validated by its ability to scale with their needs. As Wipro continues to grow and tackle increasingly sophisticated cyber threats for its customers, Binalyze AIR's scalable architecture ensures it can maintain a proactive and robust cybersecurity incident management strategy.

David elaborated: "We are servicing a large pool of clients, so scalability is a top priority for us. We're working on building out more functionality around the API so we can take AIR's automation to the next level and drive even more efficiency."

In summary, deploying Binalyze AIR transformed Wipro's incident response and cybersecurity forensics operations. The solution provided substantial efficiency gains, enhanced collaboration, and improved response times, all of which contributed to a stronger and more resilient cybersecurity posture for Wipro's global customers. By leveraging advanced automation and remote evidence acquisition, Wipro has set a new standard in managing cyber threats and ensuring comprehensive protection for its clients.