binalyze!

CYBERCLAN™
Enterprise Security. Human Response.

Incident response services provider **CyberClan** eyes significant commercial opportunities to scale thanks to **Binalyze AIR**

Company overview

Headquartered in Vancouver, CyberClan provides its global customers with first-class Incident Response & Breach Response services. The portfolio of services broadly covers cyber extortion, ransomware, e-discovery, tailored risk management consultancy services, and unparalleled managed security services.

Challenges

- Time-consuming evidence acquisitions
- Limited time to triage remote devices
- The limited scope of artifacts available

Challenges in cybersecurity forensics

When customers call CyberClan today, most are in the middle of an active incident and require quick assistance and resolution. As a remote company providing services to small security teams and having an industry-leading response time commitment of 15 minutes, there were a number of operational challenges - notably around quickly collecting data and enabling accurate post breach recovery (PBR)."

Since investigations are timebound based on a statement of work (SOW), it became increasingly important to be able to discharge their services whilst providing customers with the best and most valuable information-led insights.

Most investigations utilized several different solutions, and triaging required manual steps and was often limited to a single asset at a time. They needed a flexible solution that could be scheduled to run but also ran ad-hoc so that rapid triage could be performed.

Given time is always critical in a breach, the business acknowledged it needed to work smarter, not harder, by more quickly identifying machines with signs of compromise and IoCs and not needing such high levels of involvement from their end customers.

CyberClan wanted to lighten the dependency on their customers, giving them the flexibility to say - we're here, we're on it, leave it to us, and we'll manage all aspects for you.

CyberClan needed a solution they could quickly deploy and use to ensure data was collected easily, with support for SFTP, was forensically sound, and not tampered with.

CyberClan wanted to turbocharge the collection of triage data over both offline and remote collection scenarios - alongside looking for ways of speeding up disk imaging efforts - focusing on the evidence that matters first. They needed to move away from acquisitions taking 8 hours on average and accelerate this to facilitate doing more for their customers.

CyberClan wanted to move beyond the typical time crunch - shifting to increased automation and better prioritization to allow for more investigations per analyst, but their previous patchwork of tools was causing a speed bottleneck, preventing them from taking on more work.

Customer
CyberClan

Industry
Incident Response & Breach Response service provider

Region
Global

Founded
2003

Employees
70 - 100

Success Highlights:

- **5x quicker** management per endpoint
- **Triage at scale,** moving from the acquisition stage to triage quickly
- **Increasing caseload** capacity through efficiency
- **Support Enterprise customers** with 1,000s of endpoints

How Binalyze AIR helped

CyberClan is leveraging Binalyze AIR to help manage its wider Digital Forensics and Incident Response (DFIR) activities, with a specific focus on using AIR in ransomware cases. For the CyberClan team, it's all about getting as much relevant data as possible whilst preserving that potential evidence.

Andrew Caldwell, DFIR Lead at CyberClan, shared: "It's been so easy to get up and running with Binalyze AIR, even the agent is quickly deployed onto lots of different endpoints and performs one big slurp (acquisition).

I was able to go through this big amount of information and cross-correlate an entire domain very easily. Then if I identify something of pertinent value, I can go back and perform a full capture.

AIR solves a lot of problems but also embraces new approaches to digital forensics. It does require a subtle change of mindset coming from Blackbox forensics. I'm also relatively new to CyberClan, but I've been so impressed with Binalyze AIR I've actively encouraged former colleagues and peers to go and check it out".

Monti Sachdeva, DFIR Lead at CyberClan, went on to explain, I've been really impressed with AIR, all the way from our very first tech demo. In practice, it's helping us with the acquisition, then automatically firing up the Triage component, letting DRONE, AIR's automated evidence analyzers, give us even more intelligence.

The agent is extremely easy to deploy and use for the average user. By adding AIR to our arsenal, a single analyst can now manage many more investigations individually. It's very powerful in getting acquisitions from memory, browsers, ram, logs, and so many more destinations.

We've just started using the Investigation Hub feature (formerly Consolidated Report), and we already love it. It's dramatically improving efficiency when you need to investigate hundreds of endpoints at once, and having one unified view for the entire team is really helpful.

The Timeline feature is also proving to be indispensable in our Incident Response activity. This feature, being largely automated, helps save us more time - removing a lot of reliance on slow manual inputting and juggling of old-school Excel spreadsheet documents. AIR is quickly becoming a one-stop shop for us, keeping all activity within one single pane of glass."

Final thoughts

Binalyze AIR is such a comprehensive and powerful platform. It's supporting both industry veterans and those new analysts coming into the incident response space. AIR is spearheading CyberClan's training of new colleagues on DFIR fundamentals - with its clean and clear user interface and intuitive design harnessing a powerful depth of capabilities.

'We've recently attracted some new colleagues into CyberClan, and they've shared that a big attraction was because we're already using AIR; that's a big compliment because there's an appreciation growing in the industry for the product,'

"Having a categorization factor of artifacts and being able to pivot inwards, beyond your more traditional warnings of something looking suspicious, and giving priority order - it's just so useful. It helps us work at scale and even feels a bit like an enhanced EDR function", shared Andrew.

"We've recently attracted some new colleagues into CyberClan, and they've shared that a big attraction was because we're already using AIR; that's a big compliment because there's an appreciation growing in the industry for the product," expanded Monti.
Simon Lang, Head of Digital Forensics & Incident Response at CyberClan, concluded

"Binalyze AIR's robust capabilities in IR triage has significantly streamlined our investigative processes. It's a super intuitive and powerful analytical platform, enabling us to quickly identify, analyze, and respond to complex cyber threats.

> **"Binalyze AIR's robust capabilities in IR triage has significantly streamlined our investigative processes. It's a super intuitive and powerful analytical platform, enabling us to quickly identify, analyze, and respond to complex cyber threats. "**
>
> – Simon Lang, Head of Digital Forensics & Incident Response CyberClan.

Conclusion

The ability to quickly perform both high-level and deep analysis on various OS types and system artifacts has provided us with investigative insights that were previously unattainable.

Put simply; AIR has become an indispensable part of the team's DFIR workflow and the top choice in our tool-kit"