From Alerts to Answers:
How SecureCyber Differentiates It's MSSP Services with Binalyze

Company overview

SecureCyber is a U.S. based Managed Security Service Provider delivering managed detection and response, incident response, and proactive security services to small and mid market organizations across a range of industries. The company focuses on helping customers who lack dedicated in-house security teams improve visibility, respond to incidents quickly, and build long term cyber resilience.

This case study is based on an interview with Joe Tinney, Vice President of Cyber Operations at SecureCyber. Joe leads SecureCyber's security operations and incident response services, bringing deep hands-on experience in digital forensics, threat investigation, and SOC enablement. He works directly with customers during high impact incidents and is responsible for designing scalable security services that work in real world environments.

Challenges

- Environment is heavily restricted to contain threats
- Investigating complex incidents in restricted and damaged environments
- Investigations risk becoming slow, manual, and fragmented.

The challenge

Investigating complex incidents in restricted and damaged environments

SecureCyber is often brought in to support organizations after a compromise has already occurred. In many cases, the environment is already heavily restricted to contain the threat.

In one investigation, the customer had fully isolated their systems from each other and from the internet. The domain controller was corrupted and could not reliably boot, new user accounts could not be created, and traditional live response methods were unavailable.

This created a situation where deploying tools remotely was impossible and continuing the investigation risked becoming slow, manual, and fragmented.

For an MSSP, these conditions pose serious challenges. Investigations stall, analyst effort increases, and confidence in findings can suffer at the exact moment clarity is most needed.

The solution

Offline evidence collection and flexible investigation with Binalyze

To overcome these constraints, SecureCyber used Binalyze's offline collection capabilities to continue the investigation without network connectivity.

Rather than relying on live access, evidence was collected by connecting directly to VMware virtual hosts and passing removable media through to the affected systems. In some cases, systems were booted using an alternative operating system to allow access to data where Windows could not be started.

Once collected, the evidence was transferred back into Binalyze and analyzed using the same investigation workflows used in live environments. This allowed the team to regain visibility, identify attacker activity, and understand the full scope of compromise despite the severely constrained conditions.

Customer
SecureCyber

Industry
Cybersecurity
Incident Response

Region
USA

Founded
2015

Website
www.securecyberdefense.com/

Success Highlights:

- **Significantly improved** both operational efficiency and service quality.
- **Faster investigations,** higher confidence, and stronger service differentiation
- **Investigations can continue** even in disconnected or damaged environments.
- **The team can handle more complex cases** without relying on multiple forensic tools.

binalyze!

SECURECYBER

'The offline acquisition capability was critical. Without it, I would have been doing largely manual forensics.'

How Binalyze Is Used Today

A core platform for both reactive and proactive MSSP services.

Binalyze is now the primary forensic and investigation platform used across SecureCyber's services.

During incident response, it is used when alerts from EDR or XDR tools are insufficient or inconclusive. Binalyze enables deeper investigation, validation of alerts, and forensic level visibility that complements existing detection tools.

Beyond reactive response, SecureCyber also offers a proactive compromise assessment service powered by Binalyze. Customers are scanned on a recurring basis, critical findings are reviewed monthly, and risks are systematically reduced over time.

Binalyze is also used internally to support analyst development. SOC analysts are trained using real investigation data, helping them understand what genuine malicious behavior looks like on an endpoint rather than relying only on alerts.

' They are blown away when they see what real malicious activity actually looks like on an endpoint.'

Results

Faster investigations, higher confidence, and stronger service differentiation.

By standardizing on Binalyze, SecureCyber has significantly improved both operational efficiency and service quality. Investigations can continue even in disconnected or damaged environments. Analysts reach conclusions faster and with greater confidence. The team can handle more complex cases without relying on multiple forensic tools.

From a commercial perspective, Binalyze enables SecureCyber to offer higher tier services, extend engagements beyond incident response, and differentiate their MSSP offering in a competitive market.

'We can investigate as far as EDR allows, but it does not pick up the same things that Binalyze does.'

Broader Impact

Turning investigations into education and long term value.

Binalyze has also helped how SecureCyber communicates with customers. Instead of presenting findings as abstract alerts or reports, investigations become collaborative and educational. Customers gain a clearer understanding of attacker behavior and why certain security policies matter.

This approach helps customers improve their own security practices and strengthens long term trust between the MSSP and the organization.

'When you show customers what attacker behavior actually looks like, the security controls suddenly make sense.'

Why Binalyze

Binalyze AIR has become a cornerstone of Blackpanda's incident response operations. The platform's efficiency gains, streamlined workflows, and collaborative features have enabled them to scale their operations effectively. Incidents now typically require just one responder each, enabling the team to handle a larger volume of cases while also delivering timely and comprehensive support to their clients.

The solution also proved instrumental in meeting stringent cross-border data residency requirements, a crucial factor for Blackpanda's operations in Asia. The platform's flexible deployment options allowed them to comply with local regulations while maintaining the speed and efficiency of their investigations. This alignment with regulatory requirements, combined with the platform's scalability and cost-effectiveness, directly supported Blackpanda's mission to democratize cybersecurity by making high-quality incident response services accessible to businesses of all sizes.

Recommendation

For security teams and MSSPs, real world investigations rarely happen in ideal conditions. Systems may be isolated, access may be limited, and time pressure is often high. In these moments, investigation capabilities need to remain effective even when traditional detection and live response tools fall short. SecureCyber's experience reinforces the importance of flexibility, offline readiness, and deeper endpoint visibility to reach confident conclusions during complex incidents.

As Joe Tinney, Vice President of Cyber Operations at SecureCyber, puts it:

'You've got to remain flexible in the face of adversity and use the tools that you have.'

This mindset underpins SecureCyber's approach to incident response and long term investigation readiness.