securonix

SECURECYBER

INDUSTRY: **MANAGED SECURITY SERVICES PROVIDER (MSSP)**

LOCATION: **DAYTON, OHIO, USA**

CASE STUDY

# Built for MSSPs: How SecureCyber Uses Securonix to Deliver MDXR Across Tenants with Speed and Precision

**Challenge:** SecureCyber, a global MSSP serving high-stakes sectors like financial services, SLED, and manufacturing, was hindered by a sluggish, legacy SIEM. Investigations were slow due to delayed search results, limited support for cloud telemetry, and an inability to scale or run meaningful cross-tenant analytics. Their analysts lacked the contextual insights and operational efficiency needed to protect diverse and complex customer environments.

**Solution:** Securonix's cloud-native, multitenant SIEM enabled SecureCyber to transform its MXDR offering. With UEBA, robust API integrations, and visual dashboards, analysts gained real-time visibility and the tools to proactively detect and respond to threats. The platform's scalability, intuitive design, and rich analytics allowed SecureCyber to streamline operations and confidently expand services to new customers.

### Benefits

- **Accelerated onboarding:** Reduced setup time from a month to under a week.
- **Deeper visibility:** Unified view across cloud, firewall, and server data.
- **Efficient operations:** One analyst can manage the entire platform.
- **Market edge:** Proactive investigations, not just alert forwarding.

### Results

SecureCyber achieved 75% faster onboarding, streamlined analyst workflows, and gained full-spectrum threat visibility with Securonix.

- **75% faster** onboarding
- **Enhanced** analyst effectiveness
- **Full-spectrum** threat visibility

## The Challenge

SecureCyber, a global Managed Security Services Provider (MSSP) based in Dayton, Ohio, has built a decade-long reputation safeguarding critical infrastructure across financial services, local governments (SLED), and manufacturing. With over 20 employees and a customer base in some of the most sensitive verticals, SecureCyber offers Managed Extended Detection and Response (MXDR), compliance advisory, and managed firewall and network services.

Before adopting Securonix, SecureCyber's security operations were constrained by the limitations of their legacy SIEM solution. Slow search speeds, a lack of scalability, limited support for modern cloud telemetry, and difficulty extracting actionable insights from customer data hindered their ability to deliver timely and comprehensive threat detection and response. They sought a modern, cloud-native SIEM that could seamlessly ingest diverse data sources, support multitenancy, and provide rich analytics to empower their analysts.

To overcome these limitations, SecureCyber turned to Securonix as the backbone of their next-generation MXDR service. With its cloud-native architecture, multitenant support, and advanced analytics capabilities, Securonix empowered SecureCyber to deliver faster, more accurate threat detection and response across all customer environments. Features like User and Entity Behavior Analytics (UEBA), integrated geolocation mapping, and customizable dashboards gave analysts immediate context into user activity and threats. With robust API support and seamless ingestion of diverse telemetry from cloud, on-premises, and hybrid sources, Securonix enabled SecureCyber to scale rapidly and elevate the overall quality and responsiveness of their security operations.

**"Securonix UEBA has been a game-changer for us. We now have better visibility into our customers' Active Directory environments, and can tie firewall logs and authentication data back to users. It's transformed how we track behavior and respond to risk."**

**"With our previous SIEM, onboarding a new customer took a month. With Securonix, we can do it in under a week—with full visibility across cloud, firewall, and server data sources. That speed, combined with Securonix's multitenant architecture and rich analytics, gives us a real edge in the MSSP market."**

– **Joe Tinney, Vice President, Cyber Operations, SecureCyber**

**"SecureCyber plays a critical role in protecting the nation's critical infrastructure across key verticals. We're proud to partner with them and provide the advanced analytics, scalability, and cloud-native architecture that enable them to deliver high-impact security services at scale."**

– **Marcia Dempster, Vice President, Channel Sales-Americas, Securonix**

## Key Challenges

- **Slow Search Performance:** SecureCyber's previous legacy SIEM required 30 minutes or more to return basic search results, making investigations inefficient and time-consuming.
- **Limited Support for Cloud Data Sources:** Their previous SIEM solution lacked the ability to ingest data from key cloud-based security tools, restricting visibility into modern environments.
- **Inability to Perform Analytics or Threat Hunting:** The prior platform lacked usable dashboards, reporting capabilities, and the ability to run meaningful queries on collected data in a timely manner.
- **No Cross-Tenant Search Functionality:** The previous SIEM siloed data within individual tenants, forcing analysts to run queries separately for each customer.
- **Scalability and Integration Constraints:** The solution could not scale to meet growing data volumes and presented challenges when integrating with existing tools and services.

## Key Features Utilized

- **User and Entity Behavior Analytics (UEBA):** Enabled correlation of user activity across data sources, helping analysts detect anomalous behavior and assign meaningful risk scores to different users.
- **Cloud-Native SIEM:** Provided scalable ingestion and analysis of data from a wide variety of cloud and on-premises sources without infrastructure overhead.
- **Multitenant Environment with Cross-Tenant Search:** Allowed analysts to query data across all customer environments simultaneously, increasing investigation speed and coverage.
- **Security Command Center and Visual Dashboards:** Delivered intuitive visualizations and alert timelines that improved situational awareness and threat triage efficiency.
- **Robust API Integrations:** Enabled seamless access to telemetry data, supporting enriched investigations and tighter integration within the broader MXDR platform.

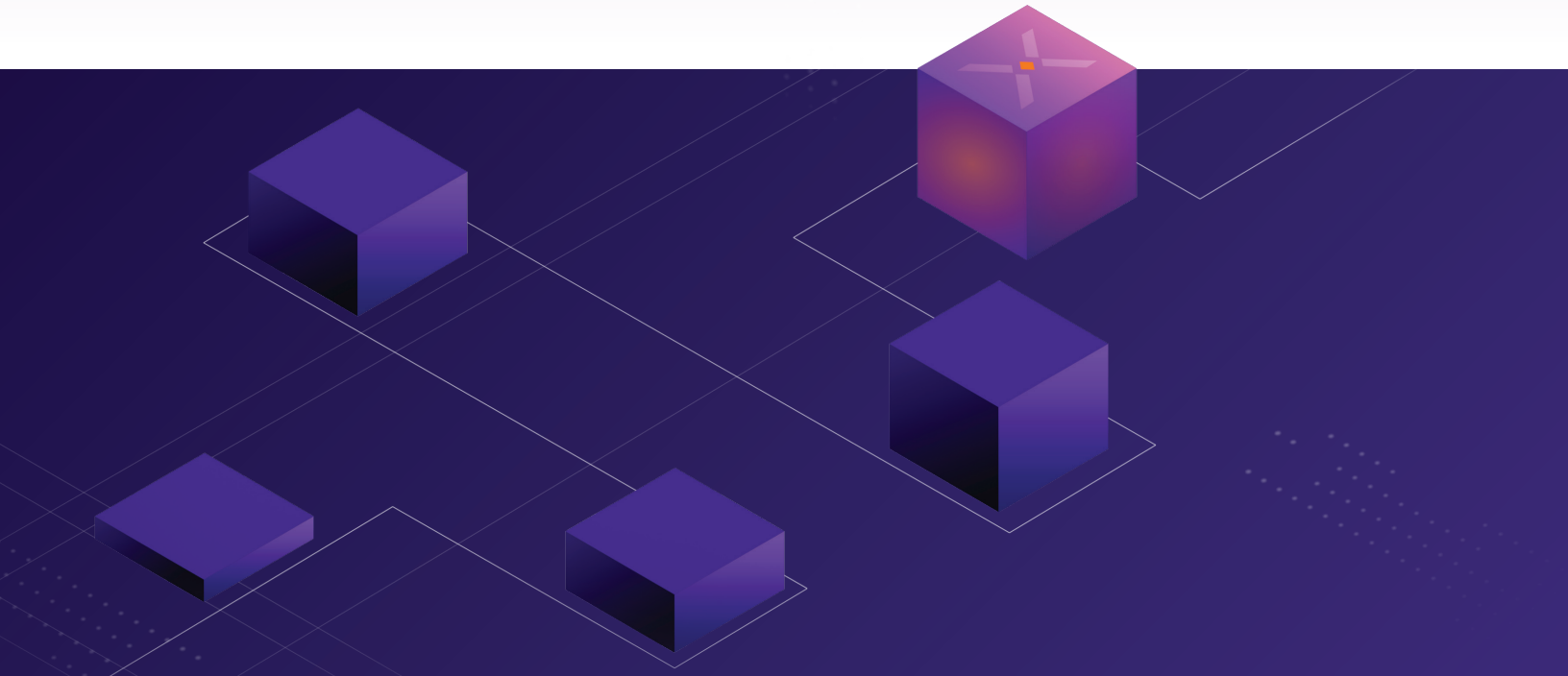
## Benefits

- **Faster Customer Onboarding:** Reduced onboarding time from approximately one month to under one week, enabling rapid service deployment across customer environments.
- **Comprehensive Visibility and Differentiated Service Delivery:** Full-spectrum visibility across cloud, firewall, and various server data sources enable proactive, analyst-led investigations that enhanced the value of SecureCyber's MXDR offering.
- **Improved Analyst Effectiveness:** Analysts gained access to enriched threat data, risk scores, and visual tools that enhanced situational awareness and investigation speed.
- **Scalable and Reliable Operations:** Confidently supported high-volume data environments without performance concerns, backed by a responsive Securonix support team.
- **Lower Operational Overhead:** Requires only one full-time employee to manage the platform, reducing staffing needs compared to managing an in-house SIEM.
- **Competitive Market Differentiation:** Delivered proactive, analyst-driven investigations and response as part of the MXDR service, rather than relying on basic alert forwarding.

## Conclusion:

By adopting Securonix, SecureCyber transitioned from a sluggish legacy SIEM to a modern, cloud-native solution that empowers its SOC team with real-time visibility, robust analytics, and rapid threat resolution capabilities. The implementation has enhanced their MXDR offerings, supported rapid customer onboarding, and positioned them to grow without worrying about infrastructure scale or complexity. Securonix's multitenant architecture, UEBA capabilities, and intuitive threat visualization have turned SecureCyber into a more agile and effective defender of critical infrastructure.

Looking forward, SecureCyber is poised to further evolve its service offerings, confident that Securonix will continue to scale with its ambitions and deliver security outcomes that matter.



### About SecureCyber

SecureCyber is a global Managed Security Services Provider (MSSP) based in Dayton, Ohio. Serving the financial, SLED, and manufacturing sectors, SecureCyber delivers Managed Extended Detection and Response (MXDR), compliance advisory, and firewall and network security services, with a mission to protect critical infrastructure.

### About Securonix

Securonix is pushing forward its mission to secure the world by staying ahead of cyber threats, reinforcing all layers of its platform with AI capabilities. Securonix Unified Defense SIEM provides organizations with the first and only AI-reinforced solution built with a cybersecurity mesh architecture on a highly scalable data cloud. The innovative cloud-native solution is enhanced by Securonix EON to deliver a frictionless CyberOps experience and enables organizations to scale up their security operations and keep up with evolving threats. For more information, visit securonix.com, or follow us on LinkedIn and X.

securonix