securonix

INDUSTRY:
FINANCIAL SERVICES

LOCATION:
AUSTRALIA

CASE STUDY

Driving Cyber Resilience with Cloud-Native SIEM: How a Global Financial Services Leader Transformed Detection and Efficiency

Challenge: A leading financial services organization managing billions in assets relied on an on-premises SIEM that created significant operational burdens. Capacity constraints, manual upgrades, and limited automation hindered proactive detection and incident response. High alert volumes, false positives, and underutilized capabilities further slowed security operations. With growing regulatory scrutiny, the organization needed a scalable, cloud-first SIEM to improve efficiency, accuracy, and resilience.

Solution: The organization implemented Securonix's Unified Defense SIEM to align with its cloud-first strategy. By eliminating infrastructure overhead, integrating UEBA and SOAR Lite, the team gained centralized visibility, automation, and advanced analytics. With 53 tuned threat models and API-driven policy lifecycle management, they improved detection accuracy, reduced manual workloads, and freed analysts to focus on higher-value security tasks.security.®

Benefits

- **Freed team from upgrades and maintenance**, improving operational efficiency
- **80% Improvement** in Mean Time to Detect (MTTD)
- **Ongoing Decline in Incident Volume** through optimized tuning

Results

- **80% faster detection speed**
- **99.98% uptime, zero downtime**

About Securonix

Securonix Unified Defense SIEM delivers AI-powered, cloud-native security operations, helping organizations stay ahead of cyber threats. Learn more at securonix.com.

The Challenge

A leading financial services organization managing billions in assets for hundreds of thousands of clients operates in a highly regulated sector and follows a "cloud-first" technology strategy to maximize efficiency and reduce operational overhead.

Previously, the company relied on an on-premises SIEM platform that created significant operational burdens. System capacity constraints, labor-intensive upgrades, and maintenance tasks limited the security team's ability to focus on proactive threat detection and incident response. In addition, the platform lacked the automation and integration capabilities needed to address an increasingly complex threat landscape.

As the Head of Cyber and Information Security, explains:

"We were struggling with capacity issues and system maintenance. On-premises upgrades were a pain that took a lot of effort and time."

Faced with growing regulatory scrutiny and evolving cyber threats, the organization needed an agile, scalable SIEM solution that could integrate seamlessly into its cloud-first environment while delivering measurable improvements in security outcomes.

The organization selected Securonix to enhance their security posture. With the help of the Securonix team, they integrated new data sources, which consolidated their organization's diverse telemetry into a single platform, effectively enhancing their visibility and threat detection capabilities. Securonix's advanced UEBA allowed them to track user behavior across their environment, reducing false positives and providing more focused alerts.

The organization achieved several critical benefits with Securonix. They significantly enhanced their visibility across their environment, allowing real-time detection of potential threats and preventing data exfiltration incidents. By fine-tuning alert policies, they reduced false positives, which improved operational efficiency and enabled their security team to focus their time and energy on more pressing activities. Additionally, by leveraging open-source threat intelligence data, they enhanced their threat detection capabilities and built customized use cases, further strengthening their security posture. Securonix also helped them improve incident response times, by providing immediate visibility into policy violations across their environment and enabling the security team to take swift action against suspicious activities.

"Quite simply, Securonix fits in perfectly with our technology strategy and cloud-first, SaaS-driven approach. It has freed up a lot of the manual work, allowing us to focus on value-added tasks and high-value security work rather than maintenance. Securonix has supported us as we've deployed new technologies, helping integrate them seamlessly and keeping us updated on new features. We need products that don't require much overhead to run, and Securonix delivers exactly that."

– **Head of Cyber and Information Security, Global Financial Services Organization**

"This partnership demonstrates how a cloud-native SIEM can drive both operational efficiency and stronger security outcomes. By aligning with their cloud-first vision, we've enabled their team to focus on proactive defense while we handle the heavy lifting behind the scenes."

– **Ajay Biyani, Vice President, Sales – APMEA, Securonix**

Key Challenges

- **System Capacity Limitations:** Hindered scalability and constrained growth potential.
- **High Manual Overhead:** Significant time spent on upgrades, patching, and maintenance tasks.
- **Limited Automation:** Slowed incident detection and response due to manual processes.
- **High Alert Volumes and False Positives:** Excessive alerts from service accounts impacting analyst efficiency.
- **Underutilized SIEM Capabilities:** Existing platform complexity limited feature adoption and value realization.
- **Policy Tuning Gaps:** Needed enhanced optimization of threat models and detection rules.

Key Features Utilized

- **Cloud-Native SIEM Platform:** Eliminated on-premises infrastructure burdens.
- **User and Entity Behavior Analytics (UEBA):** Enhanced detection of anomalous behavior.
- **SOAR Lite:** Streamlined incident workflows with automation.
- **Threat Models:** 53 enabled models aligned with MITRE ATT&CK framework.
- **Automated Policy Lifecycle:** API-driven updates and notification enhancements.
- **Zero Downtime Operations:** Maintained 99.98% uptime.

Benefits

- **Operational Efficiency:** Shifted focus from platform maintenance to proactive detection and incident handling.
- **Improved Mean Time to Detect (MTTD):** Achieved an 80% improvement in detection speed.
- **Reduced Incident Volume:** Consistent decline in incidents through better tuning. - 10% reduction over the quarter.
- **Higher True Positive Rates:** Improved accuracy of alerts, reducing false positives and analyst fatigue. - 55% increase in True Positive Rates, 10% reduction False Positives.
- **Future-Ready Security Posture:** On a clear maturity path towards AI-powered cyber defense.
- **Seamless Integration:** Embedded into the organization's evolving tech stack with continuous feature adoption.

Results

METRIC	IMPACT
Mean Time to Detect (MTTD)	Improved by 80%
Incident Volume	Decreased consistently
True Positive Rate	Increased with effective tuning
Threat Models Triggered	2 triggered; 3 new + 41 updates
System Uptime	99.98%, with 0% downtime

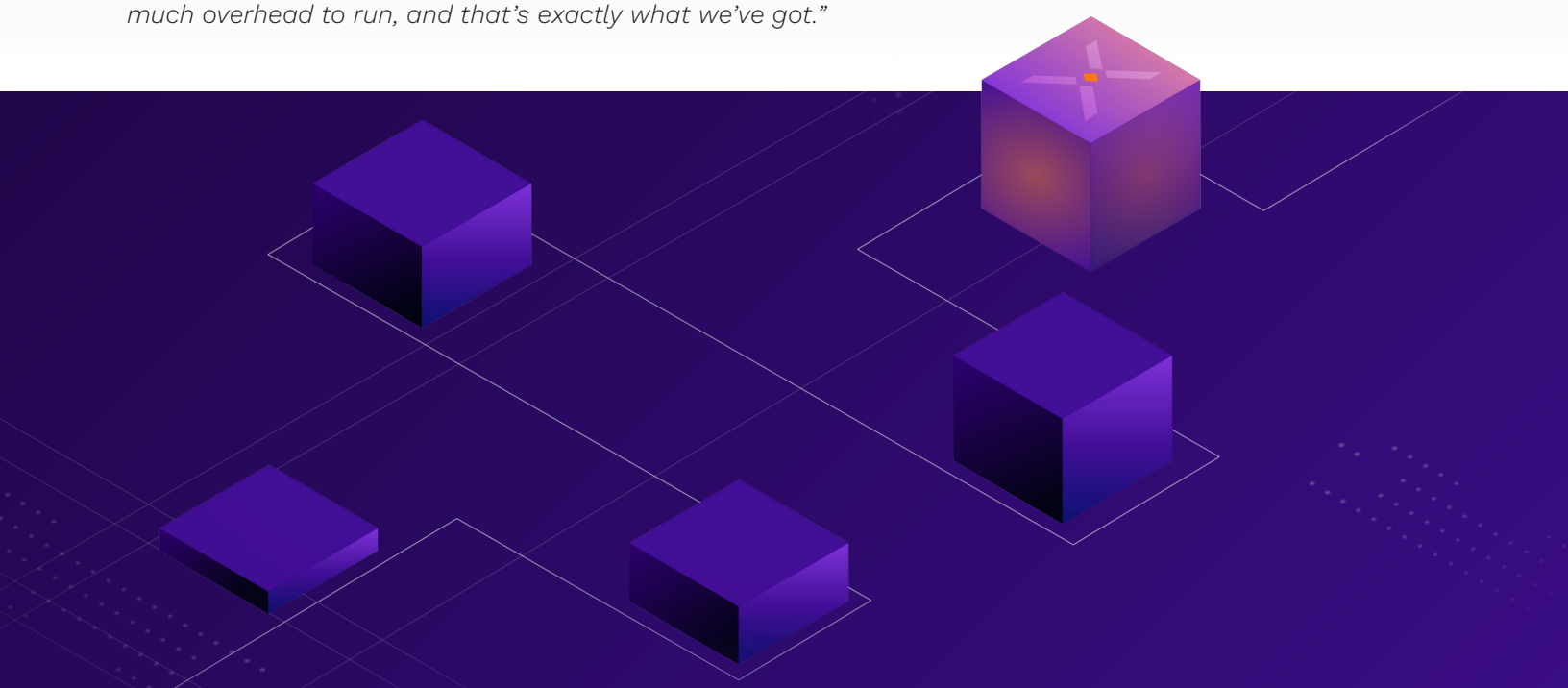
Conclusion:

By replacing its legacy on-premises SIEM with the cloud-native Securonix platform, the organization has transformed its security operations. Freed from the burden of manual maintenance, the team can now dedicate resources to high-value detection and response activities.

The integration of advanced analytics, automation, and proactive threat hunting has delivered measurable improvements in detection speed, incident accuracy, and operational efficiency. The organization is now positioned to meet regulatory requirements and combat sophisticated threats without increasing headcount or complexity.

As the Head of Cyber and Information Security notes:

"Securonix fits in perfectly with our cloud-first, SaaS-driven approach. We need products that don't require much overhead to run, and that's exactly what we've got."



About the Customer

This global financial services organization manages billions in assets on behalf of hundreds of thousands of clients. With a cloud-first technology approach, the company is committed to delivering operational efficiency and a secure environment that meets stringent industry regulations and rising customer expectations.

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 Agentic AI to deliver a frictionless SecOps 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